COMPENDIO DE LEGISLACIÓN PENAL INFORMÁTICA EN EL PERÚ

ERICK IRIARTE AHON

COMPENDIO DE LEGISLACIÓN PENAL INFORMÁTICA EN EL PERÚ

COMPENDIO DE LEGISLACIÓN PENAL INFORMÁTICA EN EL PERÚ

Erick Iriarte Ahon

Compendio de Legislación Penal Informática en el Perú
© Erick Iriarte Ahon
@CoyoteGris

Versión 1.0, Actualizado al 12.12.2024

Editado por:
© Iriarte & Asociados, S.C. de R.L.
Calle Enrique Palacios Nro. 360 Int. 612, Miraflores
Lima – Perú

Fondo Editorial de la Universidad La Salle
Av. Alfonso Ugarte 517, Cercado
Arequipa – Perú

Diseño, diagramación y carátula:
Carlos Eduardo Zúñiga Izquierdo

Primera edición: marzo 2025
ISBN en trámite

Hecho el Depósito Legal en la Biblioteca Nacional del Perú N.º 2025-xxxxx

A quienes se dedican a la ciberdefensa, a la ciberseguridad y a combatir el cibercrimen, su esfuerzo en silencio permite que se construya un Perú Digital.

A todos los miembros de Alfa-Redi, que me enseñaron, que compartieron conmigo, que me permitieron conocer otras realidades, pero todos con el mismo espíritu de lograr una Sociedad de la Información para todos y todas.

PRÓLOGO

Es un verdadero privilegio y un honor personal *poder escribir* estas líneas para presentar el documento **Compendio de Legislación Penal Informática en el Perú**, elaborado por mi gran amigo Erick Iriarte Ahon. Nos conocemos desde que teníamos 6 años, desde las mismas bases del Colegio La Salle de Lima, y a lo largo de los años he sido testigo de su crecimiento tanto a nivel personal como profesional. Erick, con su inigualable visión, se ha consolidado como un pionero en el derecho informático, y ha sido una figura clave en el desarrollo de normativas que hoy son vitales para la protección en el entorno digital.

Desde mi experiencia en ciberseguridad, fraudes informáticos y seguridad de la información, puedo afirmar que este documento llega en un momento crucial: El panorama de amenazas digitales no deja de evolucionar, y es aquí donde el trabajo de Erick cobra una relevancia indiscutible. Esta recopilación no solo incluye las principales leyes que regulan los delitos informáticos, sino que proporciona una base sólida para que tanto las empresas privadas como las entidades públicas puedan afrontar con mayor claridad los desafíos que plantea la digitalización.

En un entorno donde los ciberataques, el acceso no autorizado a sistemas, la suplantación de identidad y el fraude informático son cada vez más comunes, la necesidad de un marco legal robusto es más que evidente. Este documento cubre aspectos esenciales como la Ley de Delitos Informáticos, el Código Penal y leyes relacionadas con la videovigilancia, la ciberdefensa y la protección de datos. Todo esto convierte al documento en una herramienta indispensable para aquellos que trabajamos en áreas críticas de la seguridad digital, tanto en el ámbito corporativo como en el sector público.

Lo que distingue esta obra es la claridad y precisión con la que presenta la información. Erick, con su vasta experiencia, ha logrado que este documento sea accesible no solo para especialistas en derecho, sino también para todos quienes necesitamos comprender cómo aplicar correctamente estas leyes en nuestra labor diaria. Esto es especialmente valioso para profesionales como yo, que diseñamos estrategias de prevención y mitigación de riesgos. El marco legal aquí expuesto nos proporciona las directrices necesarias para cumplir con las normativas vigentes y actuar con mayor efectividad.

Además, no puedo dejar de mencionar el incansable espíritu de innovación que caracteriza a Erick. Estoy seguro de que pronto escucharemos sobre nuevas iniciativas que estará impulsando, particularmente en el uso de la inteligencia artificial en los ámbitos público y privado. La inteligencia artificial ya está transformando no solo la forma en que operamos a nivel técnico, sino también cómo aplicamos las leyes y aseguramos la ética en su uso. Las discusiones sobre el impacto ético y legal de la IA son cada vez más frecuentes en foros de tecnología y ciberseguridad, y no me cabe duda de que Erick estará a la vanguardia de estas iniciativas, contribuyendo con propuestas que equilibren la innovación con la responsabilidad.

En los distintos foros de ciberseguridad y tecnología a los que asisto, las nuevas tendencias destacan la convergencia entre la inteligencia artificial y otros sistemas críticos. El impacto de la automatización y la IA en la administración de justicia y la gestión de riesgos cibernéticos es uno de los temas más discutidos. Estoy convencido de que Erick, con su profundo entendimiento del derecho y la tecnología, jugará un papel clave en estos debates, proponiendo nuevas normativas que permitan un uso adecuado de estas herramientas sin comprometer los valores éticos fundamentales.

Este documento es una muestra más de su compromiso por mantenernos al día en un campo que no deja de evolucionar.

Para aquellos que trabajamos en ciberseguridad y en el ámbito legal, esta obra es una guía indispensable que no solo refleja la situación actual, sino que nos prepara para los desafíos del futuro.

Gracias, amigo, por tu dedicación incansable y por compartir con nosotros este documento, que sin duda será de gran utilidad para todos los que buscamos construir un entorno digital más seguro y equitativo.

Alfredo Alva Lizárraga
Experto en Ciberseguridad y Seguridad de la Información
Presidente del Capitulo Peruano de *Cloud Security Alliance*

***En un mundo cada vez más digitalizado**, donde las tecnologías de la* información y la comunicación (TIC) permean todos los aspectos de nuestra vida, la necesidad de un marco legal sólido y actualizado que regule su uso se vuelve imperativa. La presente obra, **Compendio de Legislación Penal Informática en el Perú**, elaborada por Erick Iriarte Ahon, responde a esta exigencia de manera exhaustiva y rigurosa.

Este compendio se erige como una herramienta indispensable para juristas, fiscales, policías, abogados, académicos y, en general, para todos aquellos interesados en comprender el complejo entramado normativo que rige los delitos informáticos en nuestro país. La prolífica labor legislativa en este ámbito, evidenciada en la multitud de normas compiladas en esta obra, refleja la creciente importancia que se otorga a la ciberseguridad y a la protección de los derechos en el entorno digital.

El autor ha realizado un trabajo titánico al recopilar, sistematizar y analizar una amplia gama de leyes, decretos legislativos y resoluciones que conforman el marco legal de TI en el Perú. Este compendio no sólo facilita el acceso a la normativa vigente, sino que también ofrece un análisis detallado de cada norma, lo que permite comprender su alcance y aplicación práctica.

Uno de los aspectos más destacables del documento es su enfoque integral. No se limita a enumerar las normas, sino que también aborda entre otros, temas cruciales como la ciberdefensa, la confianza digital, la geolocalización, la videovigilancia y la vigilancia electrónica. Además, incluye un detallado índice de delitos informáticos, lo que facilita la búsqueda de información específica.

Este compendio constituye un valioso aporte a la comunidad jurídica y tecnológica peruana. Al poner a disposición de todos un conocimiento especializado y actualizado en materia de ciberdelincuencia tan necesario

en estas épocas de digitalización, contribuyendo a fortalecer el Estado de derecho en el ámbito digital y a garantizar una mayor seguridad en el ciberespacio.

Enhorabuena a Erick Iriarte Ahon por esta iniciativa que sin duda se convertirá en un referente obligado para todos aquellos que trabajan en la prevención y persecución de los delitos informáticos en nuestro país.

Giovanni Pichling Zolezzi
Gerente de Seguridad Estratégica, ASBANC

INTRODUCCIÓN

Cibercrimen: acción contra bienes jurídicos utilizando herramientas digitales. Se puede dividir en delitos informáticos (delitos contra el bien jurídico información) y delitos por medios informáticos (delitos que utilizan las tecnologías para su ejecución).

Para empezar, debemos definir a qué nos referimos con cibercrimen, ya que en muchos casos se confunden los delitos informáticos con el cibercrimen que, como defino en el párrafo anterior, **es solo un aspecto** del fenómeno.

La aparición de la tecnología ha facilitado la vida a las personas y les ha dado posibilidades de mejorar la sociedad, generando al mismo tiempo nuevas herramientas para aquellos quienes buscan afectarlas. El entorno digital es un reflejo de nuestro entorno presencial, pero añadiendo instrumentos de acceso remoto, además de un alcance masivo y transfronterizo.

Pero, si bien existen estas afectaciones, el derecho -y en especial el derecho penal como *ultima ratio*- ha desarrollado instrumentos para enfrentar dichas acciones, dichos ilícitos.

Este manual nos permite tener en un solo instrumento lo desarrollado a la fecha en los pasados 33 años (desde la llegada del internet al Perú de la mano de la Red Científica Peruana) en materia de *derecho penal informático*, término totalmente arbitrario que he desarrollado para abarcar este tipo de regulación.

Espero esta publicación sea un instrumento útil para la labor de todas las personas, en especial de quienes se encargan del *law enforcement* y del cumplimiento de la ley (jueces, fiscales, policías, abogados), pero tambien de académicos, desarrolladores de políticas y desarrolladores de regulación (congresistas), para que puedan tener claridad sobre qué está regulado, qué está mal regulado, qué puede mejorarse y qué no requiere ser alterado.

NORMAS INVOLUCRADAS

- Ley de Delitos Informáticos [y por medios informáticos] (y sus modificaciones)
- Código Penal
- Código Procesal Penal
- Código de Ejecución Penal
- Ley 27697, Ley que otorga facultad al fiscal para la Intervención y control de comunicaciones y documentos privados en caso excepcional
- Ley 28774, Ley que crea el Registro nacional de Terminales de Telefonía Celular, Establece Prohibiciones y Sanciona Penalmente a quienes alteren y comercialicen celulares de procedencia dudosa
- Ley 28820
- Ley 29499, Ley que establece la vigilancia electrónica personal
- Ley 29867, Ley que incorpora diversos artículos al Código Penal relativos a la Seguridad en los Centros de Detención o Reclusión
- Ley 30076, Ley para combatir la inseguridad ciudadana
- Ley 30077, Ley contra el crimen organizado
- Decreto Legislativo 982
- Decreto Legislativo 1182, Decreto que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado.
- Decreto Legislativo 1218, Regula el uso de las camaras de videovigilancia
- Ley 30618, Ley que modifica el DL 1141, DL de fortalecimiento y modernización del Sistema de Inteligencia Nacional – SINA y de la Dirección Nacional de Inteligencia, DINI, a fin de regular la seguridad digital
- DS 050-2018-PCM: Aprueban la definición de Seguridad Digital en el Ámbito Nacional
- Decreto Legislativo 1412, Ley de Gobierno Digital
- Resolución Legislativa 30913, Resolución Legislativa que aprueba el Convenio sobre la Ciberdelincuencia (Convenio de Budapest)
- Ley 3099, Ley de Ciberdefensa

- Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el marco de Confianza Digital y dispone medidas para su fortalecimiento
- DS 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo
- DS 017-2024-PCM, Reglamento de la Ley de Ciberedefensa
- Ley 32183, que modifica el Código Penal, decreto legislativo 635, para incorporar la modalidad de préstamos extorsivos en el tipo penal de extorsión

Lo primero que debemos destacar de este levantamiento de información es lo "prolíficos" que han sido los legisladores peruanos para desarrollar -de manera directa e indirecta- o modificar normativa ya existente para temas de uso de TICs en la aplicación de justicia y sobre la aplicación de la justicia en caso de malos usos de las TICs.

Lo segundo, por otra parte, es la incorporación sistemática del uso de las TICs en la aplicación de justicia en todas las fases del proceso jurídico, siendo la utilización de tecnologías como la videoconferencia facilitadoras de la labor judicial.

El desarrollo de codificación penal ha tenido dos vertientes: una pensada en la regulación de conductas, que es la que consideramos idónea, dado que la tecnología no es mas que un instrumento y no es la causa en sí de hechos punibles; y la desarrollada alrededor de la premisa de que la tecnología en sí misma es la causante del hecho punible. Ambas tendencias coexisten en el Código Penal y en la ley (mal llamada) de Delitos Informáticos.

De igual modo, queda como tarea pendiente el desarrollo normativo en materia de Informática Forense tras la adhesión al Convenio de Cibercrimen de Budapest.

Esta es una primera aproximación a un compendio normativo en la materia, que esperamos sea de utilidad para la comunidad, los actores jurídicos (jueces, fiscales, policías, abogados), los académicos y los tomadores de decisiones.

Primera Sección

GUÍA RÁPIDA

Normas referidas

Ley de Delitos Informáticos (LDI)

Código Penal (CP)

Código Procesal Penal (CPP)

Código de Ejecución Penal (CEP)

Ley que otorga facultad al fiscal para la Intervención y control de comunicaciones y documentos privados en caso excepcional (LF)

Ley contra el crimen organizado (LCO)

Ley de Geolocalización (LG)

Ley de Videovigilancia (LV)

Decreto Supremo 050-2018-PCM, Aprueba definición de seguridad digital (DSSD)

Ley de Gobierno Digital (LGD)

Ley de Ciberdefensa (LCD)

Decreto de Urgencia de Confianza Digital (DUCD)

Delitos tipíficados

Abuso de mecanismos y dispositivos informáticos: LDI art. 10, CP 220B

Acceso a Datos de Tarjetas de Banco: CP art. 196A.5

Acceso Ilícito: LDI art. 2

Acoso Sexual: CP art. 176B

Actos contra el Pudor: CP art. 176, 183

Apología del Delito: CP art. 316

Apología del Terrorismo: CP art. 316A

Atentados contra el Espectro Radioeléctrico: CP art. 186.7

Atentado contra Integridad de datos informáticos: LDI art. 3 CP 220A

Atentando contra Integridad de Sistemas Informáticos: LDI art. 4, CP 283

Atentado contra la seguridad común: CP art. 281

Atentado contra las Telecomunicaciones: CP art. 186.10, 222A, 281, 283

Atentado contra señales de satélite: CP art. 186A, 194A, 444A

Calumnia: CP art. 131

Chantaje: CP art. 201

Chantaje Sexual: CP art. 177C

Chantaje sexual con materiales elaborados o modificados por medios digitales o tecnológicos: LDI art. 5B

Delitos contra Derechos Intelectuales: CP art. 216, 217, 218, 219, 220, 220A, 220B, 220C, 220D, 220E, 220F, 222, 222A, 223

Delitos contra la administración pública (equipos electrónicos y teléfonos móviles en penales): CP art. 368A, 368B, 368C, 368D

Delitos contra la seguridad publica: CP art. 281

Delitos contra Software: CP art. 220F

Difamación: CP art. 132

Discriminación: CP art. 323

Entorpecimiento al funcionamiento de servicios públicos: CP art. 283

Espionaje: CP art. 331, 331A

Estafa / Phishing: CP art. 196, 196A

Exhibiciones y publicaciones obscenas: CP art. 183

Explotación sexual comercial infantil y adolescente en ámbito del turismo: CP art. 181A

Falsedad Ideológica: CP art. 428

Falsificación de Documentos: CP art. 427

Fraude Informático: LDI art. 8

Delito de grave perturbación de la tranquilidad pública: CP art. 315A.

Hacking Etico: LDI art. 12

Injuria: CP art. 130

Interceptación de Comunicaciones (Datos Informáticos y Telefónica): LDI art. 7, CP art 162

Interferencia de comunicaciones electrónicas, de mensajería instantánea y similares: CP art 162B

Pánico Financiero: CP art. 249

Penalización de Clonación o Adulteración de Terminales: CP art. 222A

Pornografía Infantil / Pedofilia: CP art. 176A, 182A, 183A

Posesión o Comercialización de equipos para interceptación telefónica: CP art. 162A

Préstamos informáticos extorsivos: LDI art. 8A

Proposiciones a Menores: LDI art. 5, CP art. 183B

Publicación en los medios de comunicación sobre delitos de libertad sexual contra niñas, niños y adolescentes: CP art. 182-A.

Revelación de Secretos Nacionales: CP art. 330

Suplantación de Identidad: LDI art. 9

Tocamientos, actos de connotación sexual o actos libidinosos en agravio de menores: CP art. 176A

Trafico de Datos Personales y Bases de Datos: CP art. 154A, 157

Violación de Correspondencia: CP art. 161, 163, 164

Violación de Intimidad: CP art. 154, 154B, 156,

Violación de la libertad de expresión: CP art. 169

Conceptos

Actuación Probatoria

Audiencia para Testigos: CPP art. 381.2, 381.3

Actuaciones Procesales

Audiencia: CPP art. 119A
Citaciones: CPP art. 129
Comunicación entre Autoridades: CPP art. 132.3, 132.6

Capacitación

Capacitación: LDI Quinta Complementaria

Ciberdefensa

Ley de Ciberdefensa
Reglamento de la Ley de Ciberdefensa

Colaboración Eficaz

Ámbito del Proceso: CPP art. 473.1a

Confianza Digital

DU de Confianza Digital

Comparecencia

Sistemas electrónicos de control: CPP art. 287

Cooperación Nacional e Internacional

Convenios Multilaterales: LDI Octava Complementaria

Regulación e imposición de multas por la Superintendencia de Banca, Seguros y AFP: LDI Décima Complementaria

Coordinación interinstitucional entre la Policía Nacional, el Ministerio Público y otros organismos especializados: LDI Tercera Complementaria

Cooperación Operativa: LDI Cuarta Complementaria

Regulación e imposición de multas por el Organismo Supervisor de Inversión Privada en Telecomunicaciones: LDI Undécima Complementaria

Convenio de Cibercrimen

Crimen Organizado

Consideración de Crimen Organizado: LCO art. 3.9

Detención

Grabación del Hecho: CPP art. 259

Mandato de Detención: CPP art. 261.3

Excepciones

Codificación de Pornografía infantil: LDI Primera Complementaria

Hacking Ético: LDI art. 12

Expediente Fiscal y Judicial

Seguridad del Expediente Fiscal: CPP art. 134.2

Seguridad del Expediente Judicial: CPP art. 136.2

Geolocalización

Normatividad: Decreto Legislativo 1182

Operatividad: Codigo Procesal Penal art. 230 inciso 4

Investigaciones

Agente Encubierto: LDI Segunda Complementaria

Atribuciones de la Policía: CPP art 68

Autorización para Interceptación de Correspondencia: CPP art. 226

Intervención de Comunicaciones: CPP art. 230, 231; LF art. 1

Interceptación de Correspondencia: CPP art. 227

Juzgamiento

Continuidad y Suspensión del Juicio: CPP art. 360.4

Publicidad del Juicio: CPP art. 357.2c

Medidas de Protección

Medidas de Protección: CPP art. 248.e, 248.g

Medidas de Seguridad y Buenas Prácticas

Buenas Prácticas: LDI Séptima Complementaria

Medidas de Seguridad: LDI Sexta Complementaria

Penas

Vigilancia Electrónica: CP 29A

Principios Penales

Principio de Extraterritorialidad, Principio Real o de Defensa y Principio de Personalidad Activa y Pasiva: CP art 2

Excepciones al Principio de Extraterritorialidad: CP art 4

Prueba Documental

Traducción de vídeos: CPP art. 187.3

Seguridad Digital

Ley 30618

LGD, Capítulo VI

DU de Confianza Digital

Definición: DSSD

Tecnologías aplicadas al Proceso

Email: CPP art. 129, 132.3, 161.3

Grabación de hecho unible por medio tecnológico: CPP art. 259

Sistemas de Comunicación por Internet. CPP art. 132.6

Sistemas de Seguridad de Información: CPP art. 134.2, 136.2

Videoconferencia: CPP art. 119A, 169.2, 360.4, 381.2, 381.3

Terminología

Terminología: LDI Novena Complementaria

Testimonio

Testigos fuera del País: CPP art. 169.2

Uso de Tecnología por Internos

Comunicaciones: CEP art. 37

VideoVigilancia

DL 1218

Vigilancia Electrónica Personal

Condiciones para Vigilancia Electrónica Personal: CP art. 52, CPP art. 207, CEP art. 53, 54 y 56

SEGUNDA SECCIÓN

La Legislación (textos completos)

Ley de Delitos Informáticos [y por medios informáticos] (y sus modificatorias)

Artículo 1. Objeto de la Ley

La presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidos mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.

Artículo 2. Acceso Ilícito

El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, o se excede en lo autorizado, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.

Si el agente accede deliberada e ilegítimamente, en todo o en parte, al sistema informático vulnerando las medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.

[Modificado por DL 1614]

Artículo 3. Atentado a la integridad de datos informáticos

El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.

[Modificado por Ley 30171]

Artículo 4. Atentado a la integridad de sistemas informáticos

El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso

a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.

[Modificado por Ley 30171]

Artículo 5. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos

El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para proponerle llevar a cabo cualquier acto de connotación sexual con él o con tercero, será reprimido con una pena privativa de libertad no menor de seis ni mayor de nueve años.

Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años.

En todos los casos se impone, además, la pena de inhabilitación conforme a los numerales 1, 2, 3, 4, 5, 6, 8, 9, 10 y 11 del artículo 36 del Código Penal.

[Modificado por DL 1591]

Artículo 5-A. Chantaje sexual con materiales elaborados o modificados por medios digitales o tecnológicos

El que, mediante el uso de tecnologías de la información o comunicación, amenaza o intimida a una persona, con la difusión de imágenes, materiales audiovisuales o audios elaborados o modificados por medios digitales o tecnológicos, para obtener de ella una conducta o acto de connotación sexual, será reprimido con pena privativa de la libertad no menor de dos ni mayor de cuatro años e inhabilitación, según corresponda, conforme a los incisos 5, 9, 10 y 11 del artículo 36 del Código Penal.

La pena privativa de libertad será no menor de tres ni mayor de cinco años e inhabilitación, cuando concurra cualquiera de las siguientes circunstancias:

1. La amenaza a la víctima se refiere a la difusión de imágenes, materiales audiovisuales o audios con contenido sexual en los que esta aparece o participa.

2. Cuando la víctima mantenga o haya mantenido una relación de pareja con el agente, son o han sido convivientes o cónyuges.

3. Cuando la víctima es menor de 18 años de edad.

[Incorporado por DL 1625]

Artículo 6. DEROGADO

Artículo 7. Interceptación de datos informáticos

El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la Información Pública.

La pena privativa de libertad será no menor de ocho ni mayor de diez cuando el delito comprometa la defensa, seguridad o soberanía nacionales.

Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores.

[Modificado por Ley 30171]

Artículo 8. Fraude informático

El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos, suplantación de interfaces o páginas web o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años y con sesenta a ciento veinte días-multa.

La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.

La misma pena se aplica al que intencionalmente colabora con la comisión de alguno de los supuestos de los párrafos precedentes, facilitando la transferencia de activos.

[Modificado por DL 1614]

Artículo 8-A. Préstamos informáticos extorsivos

El que a través de plataformas digitales, internet u otro medio análogo induce u obliga mediante amenaza, intimidación, engaño o ardid a aceptar dinero o bienes, simulando un contrato de mutuo o cualquier otro con el fin de obtener una ventaja indebida, será reprimido con pena privativa de libertad no menor de diez ni mayor de quince años.

La pena será no menor de quince ni mayor de veinticinco años, cuando:

a) Se ejerce violencia para obtener la ventaja indebida.

b) La víctima tiene discapacidad, tiene entre catorce y menos de dieciocho años de edad o es adulta mayor, padece de una enfermedad grave, pertenece a un pueblo

indígena u originario, o presenta cualquier situación de vulnerabilidad.

c) El agente comete el delito en el marco de la actividad de una persona jurídica.

d) La comisión del hecho punible es de carácter transnacional, de acuerdo al numeral 2 del artículo 3 de la Convención de las Naciones Unidas Contra la Delincuencia Organizada Transnacional - Convención de Palermo

[Incorporado por Ley 32183]

Artículo 9. Suplantación de identidad

El que, mediante las tecnologías digitales suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material, moral o de cualquier otra índole, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.

La pena privativa de libertad es no menor de seis ni mayor de nueve años cuando se suplante la identidad de una persona menor de 18 años de edad y resulte algún perjuicio, material, moral o de cualquier otra índole.

[Modificado por DL 1591]

Artículo 10. Abuso de mecanismos y dispositivos informáticos

El que deliberada e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.

[Modificado por Ley 30171]

Artículo 11. Agravantes

El juez aumenta la pena privativa de libertad hasta en un tercio por encima del máximo legal fijado para cualquiera de los delitos previstos en la presente Ley, cuando:

1. El agente comité el delito en calidad de integrante de una organización criminal.

2. El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.

3. El agente comete el delito con el fin de obtener un beneficio económico, salvo en los delitos que prevén dicha circunstancia.

4. El delito compromete fines asistenciales, la defensa, seguridad y soberanías nacionales.

Artículo 12. Exención de responsabilidad penal

Está exento de responsabilidad penal el que realiza las conductas descritas en los artículos 2, 3, 4 y 10 con el propósito de llevar a cabo pruebas autorizadas u otros procedimientos autorizados destinados a proteger sistemas informáticos.

[Incorporado por Ley 30171]

Disposiciones Complementarias Finales

PRIMERA. Codificación de la pornografía infantil

La Policía Nacional del Peru, puede mantener en sus archivos, con la autorización y supervisión respectiva del Ministerio Publico, material de pornografía infantil, en medios de almacenamiento de datos informáticos, para fines exclusivos del cumplimiento de su función. Para tal efecto, debe contar con una base de datos debidamente codificada. La Policía Nacional del Peru y el Ministerio Publico establecen protocolos de coordinación en el plazo de treinta días, a fin de cumplir con la disposición establecida en el párrafo anterior.

SEGUNDA. Agente encubierto en delitos informáticos

El fiscal, atendiendo a la urgencia del caso particular y con la debida diligencia, puede autorizar la actuación de agentes encubiertos a efectos de realizar las investigaciones de los delitos previstos en la presente Ley y de todo delito que se cometa mediante tecnologías de la información o de la comunicación, incluso si estas acciones deben realizarse en entornos digitales, y con prescindencia de si los mismos están vinculados a una organización criminal, de conformidad con el artículo 341 del Código Procesal Penal, aprobado mediante el Decreto Legislativo 957.

Los protocolos para la actuación del agente encubierto en entornos digitales, tanto en el marco de la presente Ley, como en el marco del artículo 341 del Código Procesal Penal, aprobado mediante el Decreto Legislativo 957, son coordinados, en cuanto corresponda, con la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en concordancia con las normas vigentes que regulan el Sistema Nacional de Transformación Digital."

[Modificado por DL 1591]

TERCERA. Coordinación interinstitucional entre la Policía Nacional, el Ministerio Público y otros organismos especializados

La Policía Nacional del Perú fortalece el órgano especializado encargado de coordinar las funciones de investigación con el Ministerio Público. A fin de establecer mecanismos de comunicación con los órganos de gobierno del Ministerio Público, la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros y los Organismos Especializados de las Fuerzas Armadas, la Policía Nacional centraliza la información aportando su experiencia en la elaboración de los programas y acciones para la adecuada persecución

de los delitos informáticos, y desarrolla programas de protección y seguridad."

[Modificado por DL 1591]

CUARTA. Cooperación operativa

Con el objeto de garantizar el intercambio de información, los equipos de investigación conjuntos, la transmisión de documentos, la interceptación de comunicaciones y demás actividades correspondientes para dar efectividad a la presente Ley, la Policía Nacional del Perú, el Ministerio Público, el Poder Judicial, el Pe-CERT (Centro de respuesta temprana del gobierno para ataques cibernéticos), la ONGEI (Oficina Nacional de Gobierno Electrónico e Informática), Organismos Especializados de las Fuerzas Armadas y los operadores del sector privado involucrados en la lucha contra los delitos informáticos deben establecer protocolos de cooperación operativa reformada en el plazo de treinta días desde la vigencia de la presente Ley.

[Modificado por Ley 30171]

QUINTA. Capacitación

Las instituciones publicas involucradas en la prevención y represión de los delitos informáticos, deben impartir cursos de capacitación destinados a mejorar la formación profesional de su personal, especialmente de la Policía Nacional del Peru, el Ministerio Publico y el Poder Judicial, en el tratamiento de los delitos previstos en la presente Ley.

SEXTA. Medidas de seguridad

La Oficina Nacional de Gobierno Electrónico e Informático (ONGEI) promueve permanentemente, en coordinación con las instituciones del sector publico, el fortalecimiento de sus medidas de seguridad para la protección de los datos informáticos sensibles y la integridad de sus sistemas informáticos.

SEPTIMA. Buenas practicas

El Estado peruano realizara acciones conjuntas con otros Estados, a fin de poner en marcha acciones y medidas concretas destinadas a combatir el fenómenos de los atraques masivos contra las infraestructuras informáticas y establecerá los mecanismos de prevención necesarios, incluyendo respuestas coordinadas e intercambio de información y buenas practicas.

OCTAVA. Convenios multilaterales

El Estado peruano promoverá la firma ratificación de convenios multilaterales que garanticen la cooperación mutua con otros Estados para la persecución de los delitos informáticos.

NOVENA. Terminología

Para efectos de la presente Ley, se entenderá, de conformidad con el Artículo 1 del Convenio sobre la Ciberdelincuencia, Budapest, 23.XI.2001:

a. Por sistema informático: todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre si, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

b. Por datos informáticos: toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informativo ejecute una función.

DECIMA. Regulación e imposición de multas por la Superintendencia de Banca, Seguros y AFP

La Superintendencia de Banca, Seguros y AFP establece la escala de multas atendiendo a las características,

complejidad y circunstancias de los casos aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 5 del Artículo 235 del código Procesal Penal, aprobado por Decreto Legislativo 957. El juez, en el termino de setenta y dos horas, pone en cocimiento del órgano supervisor la omisión incurrida por la empresa, con los recaudos correspondientes sobre las características, complejidad y circunstancias del caso particular, a fin de aplicarse la multa correspondiente.

UNDÉCIMA. Regulación e imposición de multas por el Organismo Supervisor de Inversión Privada en Telecomunicaciones

El Organismo Supervisor de Inversión Privada en Telecomunicaciones establece las multas aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 4 del artículo 230 del Código Procesal Penal, aprobado por Decreto Legislativo 957.

Las empresas de telecomunicaciones organizan sus recursos humanos y logísticos a fin de cumplir con la debida diligencia y sin dilación la obligación prevista en el numeral 4 del artículo 230 del Código Procesal Penal.

El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa a fin de que el Organismo Supervisor de Inversión Privada en Telecomunicaciones aplique la multa correspondiente.

[Modificado por Ley 30171]

Código Penal

Generales

Artículo 2. Principio de Extraterritorialidad, Principio Real o de Defensa y Principio de Personalidad Activa y Pasiva

La Ley Penal peruana se aplica a todo delito cometido en el extranjero, cuando:

1. El agente es funcionario o servidor público en desempeño de su cargo;

2. Atenta contra la seguridad o la tranquilidad pública o se traten de conductas tipificadas como lavado de activos, siempre que produzcan sus efectos en el territorio de la República;

3. Agravia al Estado y la defensa nacional; a los Poderes del Estado y el orden constitucional o al orden monetario;

4. Es perpetrado contra peruano o por peruano y el delito esté previsto como susceptible de extradición según la Ley peruana, siempre que sea punible también en el Estado en que se cometió y el agente ingresa de cualquier manera al territorio de la República;

5. El Perú está obligado a reprimir conforme a tratados internacionales.

Artículo 4. Excepciones al Principio de Extraterritorialidad

Las disposiciones contenidas en el Artículo 2, incisos 2, 3, 4 y 5, no se aplican:

1. Cuando se ha extinguido la acción penal conforme a una u otra legislación;

2. Cuando se trata de delitos políticos o hechos conexos con ellos; y,

3. Cuando el procesado ha sido absuelto en el extranjero o el condenado ha cumplido la pena o ésta se halla prescrita o remitida.

Si el agente no ha cumplido totalmente la pena impuesta, puede renovarse el proceso ante los tribunales de la República, pero se computará la parte de la pena cumplida.

Artículo 29-A. Cumplimiento de la pena de vigilancia electrónica personal

La pena de vigilancia electrónica personal se cumplirá de la siguiente forma:

1. La ejecución se realizará en el domicilio o lugar que señale el condenado, a partir del cual se determinará su radio de acción, itinerario de desplazamiento y tránsito.

2. El condenado estará sujeto a vigilancia electrónica personal para cuyo cumplimiento el juez fijará las reglas de conducta que prevé la ley, así como todas aquellas reglas que considere necesarias a fin de asegurar la idoneidad del mecanismo de control.

3. El cómputo de la aplicación de la vigilancia electrónica personal será a razón de un día de privación de libertad por un día de vigilancia electrónica personal.

4. El condenado que no haya sido anteriormente sujeto de sentencia condenatoria por delito doloso podrá acceder a la pena de vigilancia electrónica personal. Se dará prioridad a:

a) Los mayores de 65 años.

b) Los que sufran de enfermedad grave, acreditada con pericia médico legal.

c) Los que adolezcan de discapacidad física permanente que afecte sensiblemente su capacidad de desplazamiento.

d) Las mujeres gestantes dentro del tercer trimestre del proceso de gestación. Igual tratamiento tendrán durante los doce meses siguientes a la fecha del nacimiento.

e) La madre que sea cabeza de familia con hijo menor o con hijo o cónyuge que sufra de discapacidad permanente,

siempre y cuando haya estado bajo su cuidado. En ausencia de ella, el padre que se encuentre en las mismas circunstancias tendrá el mismo tratamiento.

5. El condenado deberá previamente acreditar las condiciones de su vida personal, laboral, familiar o social con un informe social y psicológico.

Artículo 36. Inhabilitación

La inhabilitación produce, según disponga la sentencia:

1. Privación de la función, cargo o comisión que ejercía el condenado, aunque provenga de elección popular;

2. Incapacidad o impedimento para obtener mandato, cargo, empleo o comisión de carácter público;

3. Suspensión de los derechos políticos que señale la sentencia;

4. Incapacidad para ejercer por cuenta propia o por intermedio de tercero profesión, comercio, arte o industria, que deben especificarse en la sentencia;

5. Incapacidad para el ejercicio de la patria potestad, tutela o curatela;

6. Suspensión o cancelación de la autorización para portar o hacer uso de armas de fuego. Incapacidad definitiva para renovar u obtener licencia o certificación de autoridad competente para portar o hacer uso de armas de fuego, en caso de sentencia por delito doloso o cometido bajo el influjo del alcohol o las drogas.

7. Suspensión, cancelación o incapacidad definitiva para obtener autorización para conducir cualquier tipo de vehículo;

8. Privación de grados militares o policiales, títulos honoríficos u otras distinciones que correspondan al cargo, profesión u oficio del que se hubiese servido el agente para cometer el delito;

9. Incapacidad definitiva para ingresar o reingresar al servicio docente o administrativo en instituciones de educación básica, centros de educación técnico-productiva, institutos o escuelas de educación superior, instituciones de educación superior artística, universidades, escuelas de las Fuerzas Armadas o de la Policía Nacional del Perú, Ministerio de Educación o sus organismos públicos adscritos, Direcciones o Gerencias Regionales de Educación, Unidades de Gestión Educativa Local y, en general, en toda institución u organismo educativo, incluyendo centros de resocialización o rehabilitación, que desarrollan actividades permanentes o temporales vinculadas a la educación, capacitación y formación sobre cualquier materia, incluyendo los ámbitos deportivo, artístico y cultural; así como, para ejercer actividad, profesión, ocupación u oficio que implique la enseñanza, el cuidado, vigilancia o atención de niñas, niños o adolescentes o del alumnado de educación superior tanto técnica como universitaria; respecto de las personas condenadas con sentencia consentida o ejecutoriada, incluido el grado de tentativa, por cualquiera de los siguientes delitos:

a) Delitos de terrorismo tipificados en el Decreto Ley Nº 25475 y delito de apología del terrorismo tipificado en el artículo 316-A del Código Penal.

b) Delitos de violación de la libertad sexual tipificados en el Capítulo IX del Título IV del Libro Segundo del Código Penal.

c) Delitos de proxenetismo tipificados en el Capítulo X del Título IV del Libro Segundo del Código Penal.

d) Delito de pornografía infantil tipificado en el artículo 183 A del Código Penal.

e) Delito de proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos tipificado en el artículo 5 de la Ley Nº 30096.

f) Delito de trata de personas y sus formas agravadas, tipificados en los artículos 153 y 153-A del Código Penal.

g) Delito de explotación sexual y sus formas agravadas tipificados en el artículo 153-B del Código Penal.

h) Delito de esclavitud y otras formas de explotación y sus formas agravadas, tipificados en el artículo 153-C del Código Penal.

i) Delitos de tráfico ilícito de drogas de la Sección Segunda del Capítulo III del Título XII del Libro Segundo del Código Penal.

j) Delitos de homicidio simple y calificado tipificados en los artículos 106, 108 y 108-A del Código Penal.

k) Delito de parricidio tipificado en el artículo 107 del Código Penal.

l) Delito de feminicidio y sus formas agravadas tipificados en el artículo 108-B del Código Penal.

m) Delito de sicariato y sus formas agravadas tipificados en el artículo 108-C del Código Penal.

n) Delito de secuestro y sus formas agravadas tipificados en el artículo 152 del Código Penal.

o) Delito de secuestro extorsivo y sus formas agravadas tipificados en el artículo 200 del Código Penal.

p) Delitos contra la humanidad (genocidio, desaparición forzada y tortura) tipificados en los capítulos I, II y III del Título XIV-A del Libro Segundo del Código Penal.

q) Delito de violación de la intimidad, por difusión de imágenes, materiales audiovisuales o audios con contenido sexual, y sus formas agravadas, tipificado en el artículo 154-B del Código Penal."

10. Privación del derecho a residir en determinados lugares o acudir a ellos;

11. Prohibición de aproximarse o comunicarse con la víctima, sus familiares u otras personas que determine el juez; o,

12. Prohibición de comunicarse con internos o visitar establecimientos penitenciarios.

13. Incapacidad definitiva o temporal para la tenencia de animales

Artículo 52. Conversión de la pena privativa de libertad

En los casos que no fuera procedente la condena condicional o la reserva del fallo condenatorio, el juez podrá convertir la pena privativa de libertad no mayor de dos años en otra de multa, o la pena privativa de libertad no mayor de cuatro años en otra de prestación de servicios a la comunidad, o limitación de días libres, a razón de un día de privación de libertad por un día de multa, siete días de privación de libertad por una jornada de prestación de servicios a la comunidad o por una jornada de limitación de días libres.

Igualmente, el juez podrá, de oficio o a petición de parte, convertir la pena privativa de libertad en pena de vigilancia electrónica personal, a razón de un día de privación de libertad por un día de vigilancia electrónica personal, en concordancia con el inciso 3 del artículo 29-A del presente Código.

Delitos contra el Honor

Artículo 130. Injuria

El que ofende o ultraja a una persona con palabras, gestos o vías de hecho, será reprimido con prestación de servicio comunitario de diez a cuarenta jornadas o con sesenta a noventa días-multa.

Artículo 131. Calumnia

El que atribuye falsamente a otro un delito, será reprimido con noventa a ciento veinte días-multa.

Artículo 132. Difamación

El que, ante varias personas, reunidas o separadas, pero de manera que pueda difundirse la noticia, atribuye a una persona, un hecho, una cualidad o una conducta que pueda perjudicar su honor o reputación, será reprimido con pena privativa de libertad no mayor de dos años y con treinta a ciento veinte días-multa.

Si la difamación se refiere al hecho previsto en el artículo 131, la pena será privativa de libertad no menor de uno ni mayor de dos años y con noventa a ciento veinte días-multa.

Si el delito se comete por medio del libro, la prensa u otro medio de comunicación social, la pena será privativa de libertad no menor de uno ni mayor de tres años y de ciento veinte a trescientos sesenticinco días-multa.

Violación de la Libertad Personal

Artículo 151-A. Acoso

El que, de forma reiterada, continua o habitual, y por cualquier medio, vigila, persigue, hostiga, asedia o busca establecer contacto o cercanía con una persona sin su consentimiento, de modo que pueda alterar el normal desarrollo de su vida cotidiana, será reprimido con pena privativa de la libertad no menor de uno ni mayor de cuatro años, inhabilitación, según corresponda, conforme a los incisos 10 y 11 del artículo 36, y con sesenta a ciento ochenta días-multa.

La misma pena se aplica al que, por cualquier medio, vigila, persigue, hostiga, asedia o busca establecer contacto o cercanía con una persona sin su consentimiento, de modo que altere el normal desarrollo de su vida cotidiana, aun cuando la conducta no hubiera sido reiterada, continua o habitual.

Igual pena se aplica a quien realiza las mismas conductas valiéndose del uso de cualquier tecnología de la información o de la comunicación.

La pena privativa de la libertad será no menor de cuatro ni mayor de siete años, inhabilitación, según corresponda, conforme a los incisos 10 y 11 del artículo 36, y de doscientos ochenta a trescientos sesenta y cinco días-multa, si concurre alguna de las circunstancias agravantes:

1. La víctima es menor de edad, es persona adulta mayor, se encuentra en estado de gestación o es persona con discapacidad.

2. La víctima y el agente tienen o han tenido una relación de pareja, son o han sido convivientes o cónyuges, tienen vínculo parental consanguíneo o por afinidad.

3. La víctima habita en el mismo domicilio que el agente o comparten espacios comunes de una misma propiedad.

4. La víctima se encuentre en condición de dependencia o subordinación con respecto al agente.

5. La conducta se lleva a cabo en el marco de una relación laboral, educativa o formativa de la víctima.

Violación de la Intimidad

Artículo 154. Violación de la intimidad

El que viola la intimidad de la vida personal o familiar ya sea observando, escuchando o registrando un hecho, palabra, escrito o imagen, valiéndose de instrumentos, procesos técnicos u otros medios, será reprimido con pena privativa de libertad no mayor de dos años.

La pena será no menor de uno ni mayor de tres años y de treinta a ciento veinte días-multa, cuando el agente revela la intimidad conocida de la manera antes prevista.

Si utiliza algún medio de comunicación social, la pena privativa de libertad será no menor de dos ni mayor de cuatro años y de sesenta a ciento ochenta días-multa.

Artículo 154-A. Tráfico ilegal de datos personales

El que ilegítimamente comercializa o vende información no pública relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga sobre una persona natural, será reprimido con pena privativa de libertad no menor de dos ni mayor de cinco años.

Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en el párrafo anterior.

Artículo 154-B. Difusión de imágenes, materiales audiovisuales o audios con contenido sexual

El que, sin autorización, difunde, revela, publica, cede o comercializa imágenes, materiales audiovisuales, audios con contenido sexual reales, incluidos aquellos que hayan sido elaborados o modificados por medios digitales o tecnológicos, de cualquier persona, será reprimido con pena privativa de libertad no menor de dos ni mayor de cinco años y con treinta a ciento veinte díasmulta.

La pena privativa de libertad será no menor de tres ni mayor de seis años y de ciento ochenta a trescientos sesenta y cinco días-multa, cuando concurra cualquiera de las siguientes circunstancias:

1. Cuando la víctima mantenga o haya mantenido una relación de pareja con el agente, son o han sido convivientes o cónyuges.

2. Cuando para materializar el hecho utilice redes sociales o cualquier otro medio que genere una difusión masiva.

La pena privativa de libertad será no menor de seis ni mayor de diez años y con veinte a trescientos sesenta y cinco días-multa, cuando la víctima tenga menos de 18 años de edad.

La pena privativa de libertad será no menor de diez ni mayor de quince años y con cincuenta a trescientos sesenta y cinco días-multa, cuando la víctima tenga menos de 14 años de edad"

[Modificado por DL 1625]

Artículo 156. Revelación de la intimidad personal y familiar

El que revela aspectos de la intimidad personal o familiar que conociera con motivo del trabajo que prestó al agraviado o a la persona a quien éste se lo confió, será reprimido con pena privativa de libertad no mayor de un año.

Artículo 157. Uso indebido de archivos computarizados

El que, indebidamente, organiza, proporciona o emplea cualquier archivo que tenga datos referentes a las convicciones políticas o religiosas y otros aspectos de la vida íntima de una o más personas, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años.

Si el agente es funcionario o servidor público y comete el delito en ejercicio del cargo, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme al artículo 36, incisos 1, 2 y 4.

Artículo 158. Ejercicio de la acción penal

Los delitos previstos en este Capítulo son perseguibles por acción privada, salvo en el caso del delito previsto en los artículos 154-A, 154-B y 155.

[Modificado por DL 1625]

Violación Secreto de las Comunicaciones

Artículo 161. Violación de correspondencia

El que abre, indebidamente, una carta, un pliego, telegrama, radiograma, despacho telefónico u otro

documento de naturaleza análoga, que no le esté dirigido, o se apodera indebidamente de alguno de estos documentos, aunque no esté cerrado, será reprimido con pena privativa de libertad no mayor de dos años y con sesenta a noventa días-multa.

Artículo 162. Interferencia telefónica

El que, indebidamente, interviene o interfiere o escucha una conversación telefónica o similar, será reprimido con pena privativa de libertad no menor de cinco ni mayor de diez años.

La pena privativa de libertad será no menor de diez ni mayor de quince años:

1. Cuando el agente tenga la condición de funcionario o servidor público, y se impondrá ademas la inhabilitación conforme al artículo 36, incisos 1,2 y 4.

2. Cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la Información Pública

3. Cuando el delito comprometa la defensa, seguridad o soberanías nacionales.

Si el agente como el delito como integrante de una organización criminal, la pena se incrmenta hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores

Artículo 162-A. Posesión o comercialización de equipos destinados a la interceptación telefónica o similar

El que fabrica, adquiere, introduce al territorio nacional, posee o comercializa equipos o softwares destinados a interceptar ilegalmente las comunicaciones o similares, será reprimido con pena privativa de la libertad no menor de diez ni mayor de quince años.

Artículo 162-B. Interferencia de comunicaciones electrónicas, de mensajería instantánea y similares

El que, indebidamente, interviene o interfiere comunicaciones electrónicas o de mensajería instantánea o similares, será reprimido con pena privativa de libertad no menor de cinco ni mayor de diez años.

La pena privativa de libertad será no menor de diez ni mayor de quince años, cuando:

1. El agente tenga la condición de funcionario o servidor público, y se impondrá además la inhabilitación conforme al artículo 36, incisos 1, 2 y 4.

2. El delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley Nº 27806, Ley de Transparencia y Acceso a la Información Pública.

3. El delito comprometa la defensa, seguridad o soberanía nacionales.

Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores.

Artículo 163. Supresión o extravío indebido de correspondencia

El que, indebidamente, suprime o extravía de su destino una correspondencia epistolar o telegráfica, aunque no la haya violado, será reprimido con prestación de servicio comunitario de veinte a cincuentidós jornadas.

Artículo 164. Publicación indebida de correspondencia

El que publica, indebidamente, una correspondencia epistolar o telegráfica, no destinada a la publicidad, aunque le haya sido dirigida, será reprimido, si el hecho causa algún perjuicio a otro, con limitación de días libres de veinte a cincuentidós jornadas.

Violación de la Libertad de Expresión

Artículo 169. Violación de la libertad de expresión

El funcionario público que, abusando de su cargo, suspende o clausura algún medio de comunicación social o impide su circulación o difusión, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años e inhabilitación conforme al artículo 36, incisos 1 y 2.

Violación de la Libertad Sexual

Artículo 176-A. Tocamientos, actos de connotación sexual o actos libidinosos en agravio de menores

El que sin propósito de tener acceso carnal regulado en el artículo 170, realiza sobre un menor de catorce años u obliga a este a efectuar sobre sí mismo, sobre el agente o tercero, tocamientos indebidos en sus partes íntimas, actos de connotación sexual en cualquier parte de su cuerpo o actos libidinosos, será reprimido con pena privativa de libertad no menor de nueve ni mayor de quince años.

Artículo 176-B. Acoso sexual

El que, de cualquier forma, vigila, persigue, hostiga, asedia o busca establecer contacto o cercanía con una persona, sin el consentimiento de esta, para llevar a cabo actos de connotación sexual, será reprimido con pena privativa de la libertad no menor de tres ni mayor de cinco años e inhabilitación, según corresponda, conforme a los incisos 5, 9, 10 y 11 del artículo 36.

Igual pena se aplica a quien realiza la misma conducta valiéndose del uso de cualquier tecnología de la información o de la comunicación.

La pena privativa de la libertad será no menor de cuatro ni mayor de ocho años e inhabilitación, según corresponda,

conforme a los incisos 5, 9, 10 y 11 del artículo 36, si concurre alguna de las circunstancias agravantes:

1. La víctima es persona adulta mayor, se encuentra en estado de gestación o es persona con discapacidad.

2. La víctima y el agente tienen o han tenido una relación de pareja, son o han sido convivientes o cónyuges, tienen vínculo parental hasta el cuarto grado de consanguinidad o segundo de afinidad.

3. La víctima habita en el mismo domicilio que el agente o comparten espacios comunes de una misma propiedad.

4. La víctima se encuentra en condición de dependencia o subordinación con respecto al agente.

5. La conducta se lleva a cabo en el marco de una relación laboral, educativa o formativa de la víctima.

6. La víctima tiene entre catorce y menos de dieciocho años.

Artículo 176-C. Chantaje sexual

El que amenaza o intimida a una persona, por cualquier medio, incluyendo el uso de tecnologías de la información o comunicación, para obtener de ella una conducta o acto de connotación sexual, será reprimido con pena privativa de la libertad no menor de dos ni mayor de cuatro años e inhabilitación, según corresponda, conforme a los incisos 5, 9, 10 y 11 del artículo 36.

La pena privativa de libertad será no menor de tres ni mayor de cinco años e inhabilitación, según corresponda, conforme a los incisos 5, 9, 10 y 11 del artículo 36, si para la ejecución del delito el agente amenaza a la víctima con la difusión de imágenes, materiales audiovisuales o audios con contenido sexual en los que esta aparece o participa.

Artículo 177. Formas agravadas

En cualquiera de los casos de los artículos 170, 171, 172, 174, 175, 176 y 176-A:

1. Si el agente procedió con crueldad, alevosía o para degradar a la víctima, la pena privativa de libertad se incrementa en cinco años en los extremos mínimo y máximo en el respectivo delito.

2. Si los actos producen lesión grave en la víctima y el agente pudo prever ese resultado, la pena privativa de libertad será no menor de treinta ni mayor de treinta y cinco años.

3. Si los actos causan la muerte de la víctima y el agente pudo prever ese resultado, la pena será de cadena perpetua.

En los casos de los delitos previstos en los artículos 171, 172, 174, 176 y 176-A la pena se incrementa en cinco años en sus extremos mínimo y máximo si concurre cualquiera de las circunstancias establecidas en el artículo 170, segundo párrafo.

Si el agente registra cualquiera de las conductas previstas en los artículos 170, 171, 172, 174, 175, 176 y 176-A mediante cualquier medio visual, auditivo o audiovisual o la transmite mediante cualquier tecnología de la información o comunicación, la pena se incrementa en cinco años en los extremos mínimo y máximo aplicable al delito registrado o transmitido.

Ofensas al Pudor Público

Artículo 182-A. Publicación en los medios de comunicación sobre delitos de libertad sexual contra niñas, niños y adolescentes

El gerente o responsable u otro con poder de decisión sobre las publicaciones o ediciones que autorice o disponga que se difunda pornografía infantil o se publiciten actos que conlleven a la trata o la explotación sexual de niñas, niños y adolescentes será reprimido con pena privativa de libertad no menor de cuatro ni mayor de seis años, así como la pena de inhabilitación conforme al artículo 36, incisos 1, 2, 3, 4, 6, 8, 9, 10 y 11

Artículo 183. Exhibiciones y publicaciones obscenas

Será reprimido con pena privativa de libertad no menor de dos ni mayor de cuatro años el que, en lugar público, realiza exhibiciones, gestos, tocamientos u otra conducta de índole obscena.

Será reprimido con pena privativa de libertad no menor de cuatro ni mayor de seis años:

1. El que muestra, vende o entrega a un menor de dieciocho años, por cualquier medio, objetos, libros, escritos, imágenes, visuales o auditivas, que por su carácter pueden afectar su desarrollo sexual.

2. El que incita a un menor de dieciocho años a la práctica de un acto de índole sexual o le facilita la entrada a lugares con dicho propósito.

3. El administrador, vigilante o persona autorizada para controlar un cine u otro espectáculo donde se exhiban representaciones de índole sexual que permita ingresar a un menor de dieciocho años.

En todos los casos se impone, además, la pena de inhabilitación conforme al artículo 36, incisos 1, 2, 3, 4, 6, 8, 9, 10 y 11.

Artículo 183-A. Pornografía infantil

El que posee, promueve, fabrica, distribuye, exhibe, ofrece, comercializa, publicita, publica, importa o exporta por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter sexual, en los cuales participen menores de dieciocho años de edad, será sancionado con pena privativa de libertad no menor de seis ni mayor de diez años y con ciento veinte a trescientos sesenta y cinco días multa.

La pena privativa de libertad será no menor de diez ni mayor de quince años y de cincuenta a trescientos sesenta

y cinco días multa cuando:

1. La víctima tenga menos de catorce años de edad.

2. El material se difunda a través de cualquier tecnología de la información o de la comunicación o cualquier otro medio que genere difusión masiva.

3. El agente actúe como miembro o integrante de una banda u organización criminal.

En todos los casos se impone, además, la pena de inhabilitación conforme al artículo 36, incisos 1, 2, 3, 4, 5, 6, 8, 9,10 y 11.

Artículo 183-B. Proposiciones a niños, niñas y adolescentes con fines sexuales

El que contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para proponerle llevar a cabo cualquier acto de connotación sexual con él o con tercero, será reprimido con pena privativa de libertad no menor de seis ni mayor de nueve años.

Cuando la víctima tiene entre catorce y menos de dieciocho años, y medie engaño, la pena será no menor de tres ni mayor de seis años.

En todos los casos se impone, además, la pena de inhabilitación conforme al artículo 36, incisos 1, 2, 3, 4, 5, 6, 8, 9, 10 y 11

Delitos contra el Patrimonio

Artículo 185. Hurto simple

El que, para obtener provecho, se apodera ilegítimamente de un bien mueble, total o parcialmente ajeno, sustrayéndolo del lugar donde se encuentra, será reprimido con pena privativa de libertad no menor de uno ni mayor de tres años. Se equiparan a bien mueble la energía eléctrica, el gas, los hidrocarburos o sus

productos derivados, el agua y cualquier otra energía o elemento que tenga valor económico, así como el espectro electromagnético y también los recursos pesqueros objeto de un mecanismo de asignación de Límites Máximos de Captura por Embarcación.

Artículo 186. Hurto agravado

El agente será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años si el hurto es cometido:

(…)

La pena será no menor de cuatro ni mayor de ocho años si el hurto es cometido:

(…)

7. Utilizando el espectro radioeléctrico para la transmisión de señales de telecomunicación ilegales.

(…)

10. Sobre bienes que forman parte de la infraestructura o instalaciones de transportes de uso público, de sus equipos o elementos de seguridad, o de prestación de servicios públicos de saneamiento, electricidad, gas o telecomunicaciones.

(…)

Artículo 186-A. Dispositivos para asistir a la decodificación de señales de satélite portadoras de programas

El que fabrique, ensamble, modifique, importe, exporte, venda, alquile o distribuya por otro medio un dispositivo o sistema tangible o intangible, cuya función principal sea asistir en la decodificación de una señal de satélite codificada portadora de programas, sin la autorización del distribuidor legal de dicha señal, será reprimido con pena privativa de la libertad no menor de cuatro años ni mayor de ocho años y con noventa a ciento ochenta días multa.

Artículo 194-A. Distribución de señales de satélite portadoras de programas

El que distribuya una señal de satélite portadora de programas, originariamente codificada, a sabiendas que fue decodificada sin la autorización del distribuidor legal de dicha señal, será reprimido con pena privativa de la libertad no menor de dos años ni mayor de seis años y con treinta a noventa días multa.

Artículo 195 - Formas agravadas.

La pena privativa de libertad será no menor de cuatro ni mayor de seis años y de sesenta a ciento cincuenta días-multa:

(…)

2. Si se trata de equipos de informática, equipos de telecomunicación, sus componentes y periféricos.

3. Si la conducta recae sobre bienes que forman parte de la infraestructura o instalaciones de transporte de uso público, de sus equipos o elementos de seguridad, o de prestación de servicios públicos de saneamiento, electricidad o telecomunicaciones.

(…)

La pena será privativa de libertad no menor de seis ni mayor de doce años si se trata de bienes provenientes de la comisión de los delitos de robo agravado, secuestro, extorsión, trata de personas y trabajo forzoso.

Artículo 196. Estafa

El que procura para sí o para otro un provecho ilícito en perjuicio de tercero, induciendo o manteniendo en error al agraviado mediante engaño, astucia, ardid u otra forma fraudulenta, será reprimido con pena privativa de libertad no menor de uno ni mayor de seis años.

Artículo 196-A. Estafa agravada

La pena será privativa de libertad no menor de cuatro ni mayor de ocho años y con noventa a doscientos días-multa, cuando la estafa:

(…)

5. Se realice para sustraer o acceder a los datos de tarjetas de ahorro o de crédito, emitidos por el sistema financiero o bancario."

Artículo 200. Extorsión

El que mediante violencia o amenaza obliga a una persona o a una institución pública o privada a otorgar al agente o a un tercero una ventaja económica indebida u otra ventaja de cualquier otra índole, será reprimido con pena privativa de libertad no menor de diez ni mayor de quince años.

La misma pena se aplicará al que, con la finalidad de contribuir a la comisión del delito de extorsión, suministra información que haya conocido por razón o con ocasión de sus funciones, cargo u oficio o proporciona deliberadamente los medios para la perpetración del delito.

El que mediante violencia o amenaza, toma locales, obstaculiza vías de comunicación o impide el libre tránsito de la ciudadanía o perturba el normal funcionamiento de los servicios públicos o la ejecución de obras legalmente autorizadas, con el objeto de obtener de las autoridades cualquier beneficio o ventaja económica indebida u otra ventaja de cualquier otra índole, será sancionado con pena privativa de libertad no menor de cinco ni mayor de diez años.

El funcionario público con poder de decisión o el que desempeña cargo de confianza o de dirección que, contraviniendo lo establecido en el artículo 42 de la Constitución Política del Perú, participe en una huelga con el objeto de obtener para sí o para terceros cualquier beneficio o ventaja económica indebida u otra ventaja de

cualquier otra índole, será sancionado con inhabilitación conforme a los incisos 1 y 2 del artículo 36 del Código Penal.

La pena será no menor de quince ni mayor de veinticinco años e inhabilitación conforme a los numerales 4 y 6 del artículo 36, si la violencia o amenaza es cometida:

(…)

b) Participando dos o más personas; o,

c) Contra el propietario, responsable o contratista de la ejecución de una obra de construcción civil pública o privada, o de cualquier modo, impidiendo, perturbando, atentando o afectando la ejecución de la misma.

(…)

Si el agente con la finalidad de obtener una ventaja económica indebida o de cualquier otra índole, mantiene en rehén a una persona, la pena será no menor de veinte ni mayor de treinta años.

(…)

Artículo 201. Chantaje

El que, haciendo saber a otro que se dispone a publicar, denunciar o revelar un hecho o conducta cuya divulgación puede perjudicarlo personalmente o a un tercero con quien esté estrechamente vinculado, trata de determinarlo o lo determina a comprar su silencio, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ciento ochenta a trescientos sesenticinco días-multa.

Artículo 205. Daño simple

El que daña, destruye o inutiliza un bien, mueble o inmueble, total o parcialmente ajeno, será reprimido con pena privativa de libertad no mayor de tres años y con treinta a sesenta días-multa."

Artículo 206. Formas agravadas

La pena para el delito previsto en el artículo 205 será privativa de libertad no menor de uno ni mayor de seis años cuando:

(…)

2. Recae sobre medios o vías de comunicación, diques o canales o instalaciones destinadas al servicio público.

(…)

6. Recae sobre infraestructura o instalaciones de transporte de uso público, de sus equipos o elementos de seguridad, o de prestación de servicios públicos de saneamiento, electricidad o telecomunicaciones.

Delitos contra los Derechos Intelectuales

Artículo 216. Copia o reproducción no autorizada

Será reprimido con pena privativa de la libertad no menor de dos ni mayor de cuatro años y de diez a sesenta días-multa, a quien estando autorizado para publicar una obra, lo hiciere en una de las formas siguientes:

a. Sin mencionar en los ejemplares el nombre del autor, traductor, adaptador, compilador o arreglador.

b. Estampe el nombre con adiciones o supresiones que afecte la reputación del autor como tal, o en su caso, del traductor, adaptador, compilador o arreglador.

c. Publique la obra con abreviaturas, adiciones, supresiones, o cualquier otra modificación, sin el consentimiento del titular del derecho.

d. Publique separadamente varias obras, cuando la autorización se haya conferido para publicarlas en conjunto; o las publique en conjunto, cuando solamente se le haya autorizado la publicación de ellas en forma separada.

Artículo 217. Reproducción, difusión, distribución y circulación de la obra sin la autorización del autor

Será reprimido con pena privativa de libertad no menor de dos ni mayor de seis años y con treinta a noventa días-multa, el que con respecto a una obra, una interpretación o ejecución artística, un fonograma o una emisión o transmisión de radiodifusión, o una grabación audiovisual o una imagen fotográfica expresada en cualquier forma, realiza alguno de los siguientes actos sin la autorización previa y escrita del autor o titular de los derechos:

a. La modifique total o parcialmente.

b. La distribuya mediante venta, alquiler o préstamo público.

c. La comunique o difunda públicamente, transmita o retransmita por cualquiera de los medios o procedimientos reservados al titular del respectivo derecho.

d. La reproduzca, distribuya o comunique en mayor número que el autorizado por escrito.

La pena será no menor de cuatro años ni mayor de ocho y con sesenta a ciento veinte días multa, cuando el agente la reproduzca total o parcialmente, por cualquier medio o procedimiento y si la distribución se realiza mediante venta, alquiler o préstamo al público u otra forma de transferencia de la posesión del soporte que contiene la obra o producción que supere las dos (2) Unidades Impositivas Tributarias, en forma fraccionada, en un solo acto o en diferentes actos de inferior importe cada uno

Artículo 218. Formas agravadas

La pena será privativa de libertad no menor de cuatro ni mayor de ocho años y con noventa a ciento ochenta días multa cuando:

a. Se dé a conocer al público una obra inédita o no divulgada, que haya recibido en confianza del titular

del derecho de autor o de alguien en su nombre, sin el consentimiento del titular.

b. La reproducción, distribución o comunicación pública se realiza con fines comerciales u otro tipo de ventaja económica, o alterando o suprimiendo el nombre o seudónimo del autor, productor o titular de los derechos.

c. Conociendo el origen ilícito de la copia o reproducción, la distribuya al público, por cualquier medio, la almacene, oculte, introduzca en el país o la saque de éste.

d. Se fabrique, ensamble, importe, exporte, modifique, venda, alquile, ofrezca para la venta o alquiler, o ponga de cualquier otra manera en circulación dispositivos, sistemas tangibles o intangibles, esquemas o equipos capaces de soslayar otro dispositivo destinado a impedir o restringir la realización de copias de obras, o a menoscabar la calidad de las copias realizadas, o capaces de permitir o fomentar la recepción de un programa codificado, radiodifundido o comunicado en otra forma al público, por aquellos que no están autorizados para ello.

e. Se inscriba en el Registro del Derecho de Autor la obra, interpretación, producción o emisión ajenas, o cualquier otro tipo de bienes intelectuales, como si fueran propios, o como de persona distinta del verdadero titular de los derechos.

Artículo 219. Plagio

Será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años y noventa a ciento ochenta días multa, el que con respecto a una obra, la difunda como propia, en todo o en parte, copiándola o reproduciéndola textualmente, o tratando de disimular la copia mediante ciertas alteraciones, atribuyéndose o atribuyendo a otro, la autoría o titularidad ajena.

Artículo 220. Formas agravadas

Será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años y noventa a trescientos sesenticinco días-multa:

a. Quien se atribuya falsamente la calidad de titular originario o derivado, de cualquiera de los derechos protegidos en la legislación del derecho de autor y derechos conexos y, con esa indebida atribución, obtenga que la autoridad competente suspenda el acto de comunicación, reproducción o distribución de la obra, interpretación, producción, emisión o de cualquier otro de los bienes intelectuales protegidos.

b. Quien realice actividades propias de una entidad de gestión colectiva de derecho de autor o derechos conexos, sin contar con la autorización debida de la autoridad administrativa competente.

c. El que presente declaraciones falsas en cuanto certificaciones de ingresos; asistencia de público; repertorio utilizado; identificación de los autores; autorización supuestamente obtenida; número de ejemplares producidos, vendidos o distribuidos gratuitamente o toda otra adulteración de datos susceptible de causar perjuicio a cualquiera de lo titulares del derecho de autor o conexos.

d. Si el agente que comete el delito integra una organización destinada a perpetrar los ilícitos previstos en el presente capítulo.

e. Si el agente que comete cualquiera de los delitos previstos en el presente capítulo, posee la calidad de funcionario o servidor público.

Artículo 220-A. Elusión de medida tecnológica efectiva

El que, con fines de comercialización u otro tipo de ventaja económica, eluda sin autorización cualquier medida tecnológica efectiva que utilicen los productores de fonogramas, artistas, intérpretes o ejecutantes, así como

los autores de cualquier obra protegida por derechos de propiedad intelectual, será reprimido con pena privativa de libertad no mayor de dos años y de diez a sesenta días multa.

Artículo 220-B. Productos destinados a la elusión de medidas tecnológicas

El que, con fines de comercialización u otro tipo de ventaja económica, fabrique, importe, distribuya, ofrezca al público, proporcione o de cualquier manera comercialice dispositivos, productos o componentes destinados principalmente a eludir una medida tecnológica que utilicen los productores de fonogramas, artistas intérpretes o ejecutantes, así como los autores de cualquier obra protegida por derechos de propiedad intelectual, será reprimido con pena privativa de libertad no mayor de dos años y de diez a sesenta días-multa.

Artículo 220-C. Servicios destinados a la elusión de medidas tecnológicas

El que, con fines de comercialización u otro tipo de ventaja económica, brinde u ofrezca servicios al público destinados principalmente a eludir una medida tecnológica efectiva que utilicen los productores de fonogramas, artistas intérpretes o ejecutantes, así como los autores de cualquier obra protegida por derechos de propiedad intelectual, será reprimido con pena privativa de libertad no mayor de dos años y de diez a sesenta días-multa.

Artículo 220-D. Delitos contra la información sobre gestión de derechos

El que, sin autorización y con fines de comercialización u otro tipo de ventaja económica, suprima o altere, por sí o por medio de otro, cualquier información sobre gestión de derechos, será reprimido con pena privativa de libertad no mayor de dos años y de diez a sesenta días-multa.

La misma pena será impuesta al que distribuya o importe para su distribución información sobre gestión de derechos, a sabiendas que esta ha sido suprimida o alterada sin autorización; o distribuya, importe para su distribución, transmita, comunique o ponga a disposición del público copias de las obras, interpretaciones o ejecuciones o fonogramas, a sabiendas que la información sobre gestión de derechos ha sido suprimida o alterada sin autorización."

Artículo 220-E. Etiquetas, carátulas o empaques

El que fabrique, comercialice, distribuya, almacene, transporte, transfiera o de otra manera disponga con fines comerciales u otro tipo de ventaja económica etiquetas o carátulas no auténticas adheridas o diseñadas para ser adheridas a un fonograma, copia de un programa de ordenador, documentación o empaque de un programa de ordenador o a la copia de una obra cinematográfica o cualquier otra obra audiovisual, será reprimido con pena privativa de libertad no menor de tres años ni mayor de seis años y de y de sesenta a ciento veinte días multa.

Artículo 220-F. Manuales, licencias u otra documentación, o empaques no auténticos relacionados a programas de ordenador

El que elabore, comercialice, distribuya, almacene, transporte, transfiera o de otra manera disponga con fines comerciales u otro tipo de ventaja económica manuales, licencias u otro tipo de documentación, o empaques no auténticos para un programa de ordenador, será reprimido con pena privativa de libertad no menor de cuatro años ni mayor de seis años y de sesenta a ciento veinte días multa

Artículo 222. Fabricación o uso no autorizado de patente

Será reprimido con pena privativa de libertad no menor de dos ni mayor de cinco años, con sesenta a trescientos

sesenta y cinco días multa e inhabilitación conforme al Artículo 36 inciso 4) tomando en consideración la gravedad del delito y el valor de los perjuicios ocasionados, quien en violación de las normas y derechos de propiedad industrial, almacene, fabrique, utilice con fines comerciales, oferte, distribuya, venda, importe o exporte, en todo o en parte:

a. Un producto amparado por una patente de invención o un producto fabricado mediante la utilización de un procedimiento amparado por una patente de invención obtenidos en el país;

b. Un producto amparado por un modelo de utilidad obtenido en el país;

c. Un producto amparado por un diseño industrial registrado en el país;

d. Una obtención vegetal registrada en el país, así como su material de reproducción, propagación o multiplicación;

e. Un esquema de trazado (tipografía) registrado en el país, un circuito semiconductor que incorpore dicho esquema de trazado (topografía) o un artículo que incorpore tal circuito semiconductor;

f. Un producto o servicio que utilice una marca no registrada idéntica o similar a una marca registrada en el país.

Artículo 222-A. Penalización de la clonación o adulteración de terminales de telefonía celular

Será reprimido con pena privativa de libertad no menor de cuatro (4) ni mayor de seis (6) años, con sesenta (60) a trescientos sesenta y cinco (365) días multa, el que altere, reemplace, duplique o de cualquier modo modifique un número de línea, o de serie electrónico, o de serie mecánico de un terminal celular, o de IMEI electrónico o físico de modo tal que pueda ocasionar perjuicio al titular, al usuario del mismo, a terceros o para ocultar la identidad de los que realizan actos ilícitos

Artículo 223. Uso o venta no autorizada de diseño o modelo industrial

Serán reprimidos con pena privativa de la libertad no menor de dos ni mayor de cinco años, con sesenta a trescientos sesenta y cinco días-multa e inhabilitación conforme al Artículo 36 inciso 4) tomando en consideración la gravedad del delito y el valor de los perjuicios ocasionados, quienes en violación de las normas y derechos de propiedad industrial:

a. Fabriquen, comercialicen, distribuyan o almacenen etiquetas, sellos o envases que contengan marcas registradas;

b. Retiren o utilicen etiquetas, sellos o envases que contengan marcas originales para utilizarlos en productos de distinto origen; y

c. Envasen y/o comercialicen productos empleando envases identificados con marcas cuya titularidad corresponde a terceros.

Delitos contra el orden financiero y monetario

Artículo 249. Pánico Financiero

El que a sabiendas produce alarma en la población propalando noticias falsas atribuyendo a una empresa del sistema financiero, a una empresa del sistema de seguros, a una sociedad administradora de fondos mutuos de inversión en valores o de fondos de inversión, a una administradora privada de fondos de pensiones u otra que opere con fondos del público, o a una cooperativa de ahorro y crédito que solo opera con sus socios y que no está autorizada a captar recursos del público u operar con terceros, inscrita en el Registro Nacional de Cooperativas de Ahorro y Crédito No Autorizadas a Captar Recursos del Público, cualidades o situaciones de riesgo que generen el peligro de retiros masivos de depósitos o el traslado o la redención de instrumentos financieros de ahorro o de

inversión, es reprimido con pena privativa de la libertad no menor de tres ni mayor de seis años y con ciento ochenta a trescientos sesenta y cinco días-multa.

La pena es no menor de cuatro ni mayor de ocho años y de trescientos sesenta a setecientos veinte días-multa si el agente es miembro del directorio o consejo de administración, gerente o funcionario de una empresa del sistema financiero, de una empresa del sistema de seguros, de una sociedad administradora de fondos mutuos de inversión en valores o de fondos de inversión, de una administradora privada de fondos de pensiones u otra que opere con fondos del público, o de una cooperativa de ahorro y crédito que solo opera con sus socios y que no está autorizada a captar recursos del público u operar con terceros, inscrita en el Registro Nacional de Cooperativas de Ahorro y Crédito No Autorizadas a Captar Recursos del Público; o si es miembro del directorio o gerente de una empresa auditora, de una clasificadora de riesgo u otra que preste servicios a alguna de las empresas antes señaladas, o si es funcionario del Ministerio de Economía y Finanzas, el Banco Central de Reserva del Perú, la Superintendencia de Banca, Seguros y AFP o la Superintendencia del Mercado de Valores.

La pena prevista en el párrafo anterior se aplica también a los ex funcionarios del Ministerio de Economía y Finanzas, el Banco Central de Reserva del Perú, la Superintendencia de Banca, Seguros y AFP o la Superintendencia del Mercado de Valores, siempre que hayan cometido delito dentro de los seis años posteriores a la fecha de su cese.

Delitos contra la seguridad pública

Artículo 281. Atentado contra la seguridad común

Será reprimido con pena privativa de libertad no menor de seis ni mayor de diez años, el que crea un peligro para la seguridad común, realizando cualquiera de las conductas siguientes:

(…)

2. Atenta contra la seguridad de los medios de telecomunicación pública o puestos al servicio de la seguridad de transportes destinados al uso público.

(…)

Artículo 283. Entorpecimiento al funcionamiento de servicios públicos

El que, sin crear una situación de peligro común, impide, estorba o entorpece el normal funcionamiento del transporte o de los servicios públicos de telecomunicaciones, saneamiento, electricidad, hidrocarburos o de sustancias energéticas similares, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de seis años."

En los casos en que el agente actúe con violencia y atente contra la integridad física de las personas o cause grave daño a la propiedad pública o privada, la pena privativa de la libertad será no menor de seis ni mayor de ocho años.

Delitos contra la paz pública

Artículo 315-A. Delito de grave perturbación de la tranquilidad pública

El que perturbe gravemente la paz pública usando cualquier medio razonable capaz de producir alarma, será sancionado con pena privativa de libertad no menor de tres ni mayor de seis años.

Se considera perturbación grave a todo acto por el cual se difunda o ponga en conocimiento de la autoridad pública, medios de comunicación social o de cualquier otro por el cual pueda difundirse masivamente la noticia, la inminente realización de un hecho o situación falsa o inexistente, relacionado con un daño o potencial daño a la vida e integridad de las personas o de bienes públicos o privados.

Si el agente actúa en calidad de integrante de una organización criminal que, para lograr sus fines, cualesquiera que sean, utiliza como medio la amenaza de la comisión del delito de terrorismo, será sancionado con pena privativa de libertad no menor de seis ni mayor de diez años.

Artículo 316. Apología

El que públicamente exalta, justifica o enaltece un delito o a la persona condenada por sentencia firme como autor o partícipe, será reprimido con pena privativa de libertad no menor de un año ni mayor de cuatro años.

Si la exaltación, justificación o enaltecimiento se hace de delito previsto en los artículos 152 al 153-A, 200, 273 al 279-D, 296 al 298, 315, 317, 318-A, 325 al 333, 346 al 350 o de los delitos de lavado de activos, o de la persona que haya sido condenada por sentencia firme como autor o partícipe, la pena será no menor de cuatro años ni mayor de seis años, doscientos cincuenta días multa, e inhabilitación conforme a los incisos 2, 4 y 8 del artículo 36 del Código Penal.

Artículo 316-A. Apología del delito de terrorismo

Si la exaltación, justificación o enaltecimiento se hace del delito de terrorismo o de cualquiera de sus tipos, o de la persona que haya sido condenada por sentencia firme como autor o partícipe, la pena será no menor de cuatro años ni mayor de ocho años, trescientos días multa e inhabilitación conforme a los incisos 2, 4, 6 y 8 del artículo 36 del Código Penal.

Si la exaltación, justificación o enaltecimiento del delito de terrorismo se realiza: a) en ejercicio de la condición de autoridad, docente o personal administrativo de una institución educativa, o b) utilizando o facilitando la presencia de menores de edad, la pena será no menor de seis años ni mayor de diez años e inhabilitación, conforme a los incisos 1, 2, 4 y 9 del artículo 36 del Código Penal.

Si la exaltación, justificación o enaltecimiento se propaga mediante objetos, libros, escritos, imágenes visuales o audios, o se realiza a través de imprenta, radiodifusión u otros medios de comunicación social o mediante el uso de tecnologías de la información o de la comunicación, del delito de terrorismo o de la persona que haya sido condenada por sentencia firme como autor o partícipe de actos de terrorismo, la pena será no menor de ocho años ni mayor de quince años e inhabilitación, conforme a los incisos 1, 2, 4 y 9 del artículo 36 del Código Penal.

Delitos contra la Humanidad

Artículo 323. Discriminación e incitación a la discriminación

El que, por sí o mediante terceros, realiza actos de distinción, exclusión, restricción o preferencia que anulan o menoscaban el reconocimiento, goce o ejercicio de cualquier derecho de una persona o grupo de personas reconocido en la ley, la Constitución o en los tratados de derechos humanos de los cuales el Perú es parte, basados en motivos raciales, religiosos, nacionalidad, edad, sexo, orientación sexual, identidad de género, idioma, identidad étnica o cultural, opinión, nivel socio económico, condición migratoria, discapacidad, condición de salud, factor genético, filiación, o cualquier otro motivo, será reprimido con pena privativa de libertad no menor de dos ni mayor de tres años, o con prestación de servicios a la comunidad de sesenta a ciento veinte jornadas.

Si el agente actúa en su calidad de servidor civil, o se realiza el hecho mediante actos de violencia física o mental, a través de internet u otro medio análogo, la pena privativa de libertad será no menor de dos ni mayor de cuatro años e inhabilitación conforme a los numerales 1 y 2 del artículo 36.

Delitos contra el Estado y la Defensa Nacional

Artículo 330. Revelación de secretos nacionales

El que revela o hace accesible a un Estado extranjero o a sus agentes o al público, secretos que el interés de la República exige guardarlos, será reprimido con pena privativa de libertad no menor de cinco ni mayor de quince años.

Si el agente obra por lucro o por cualquier otro móvil innoble, la pena será no menor de diez años.

Cuando el agente actúa por culpa, la pena será no mayor de cuatro años.

Artículo 331. Espionaje

El que espía para comunicar o comunica o hace accesibles a un Estado extranjero o al público, hechos, disposiciones u objetos mantenidos en secreto por interesar a la defensa nacional, será reprimido con pena privativa de libertad no menor de quince años.

Si el agente obró por culpa la pena será no mayor de cinco años.

Artículo 331-A. Espionaje

El que por cualquier medio revela, reproduce, exhibe, difunde o hace accesible en todo o en parte, el contenido de información y/o actividades secretas del Sistema de Defensa Nacional, será reprimido con pena privativa de libertad no menor de cinco ni mayor de diez años e inhabilitación de conformidad con el artículo 36, incisos 1, 2, y 4 de este Código.

El que proporcione o haga accesible a terceros, sin la autorización pertinente, las informaciones y/o actividades a que se refiere el párrafo anterior, será reprimido con pena privativa de libertad no menor de seis ni mayor de doce años e inhabilitación de conformidad con el artículo 36, incisos 1, 2, y 4 de este Código.

Delitos contra la administración pública

Artículo 368-A. Ingreso indebido de equipos o sistema de comunicación, fotografía y/o filmación en centros de detención o reclusión

> El que indebidamente ingresa, intenta ingresar o permite el ingreso a un centro de detención o reclusión, equipos o sistema de comunicación, fotografía y/o filmación o sus componentes que permitan la comunicación telefónica celular o fija, radial, vía internet u otra análoga del interno, así como el registro de tomas fotográficas, de video, o proporcionen la señal para el acceso a internet desde el exterior del establecimiento penitenciario será reprimido con pena privativa de libertad no menor de cuatro ni mayor de seis años.
>
> Si el agente se vale de su condición de autoridad, abogado defensor, servidor o funcionario público para cometer o permitir que se cometa el hecho punible descrito, la pena privativa será no menor de seis ni mayor de ocho años e inhabilitación, conforme al artículo 36, incisos 1 y 2, del presente Código.

Artículo 368-B. Ingreso indebido de materiales o componentes con fines de elaboración de equipos de comunicación en centros de detención o reclusión

> El que indebidamente ingresa, intenta ingresar o permite el ingreso a un centro de detención o reclusión, materiales o componentes que puedan utilizarse en la elaboración de antenas, receptores u otros equipos que posibiliten o faciliten la comunicación telefónica celular o fija, radial, vía internet u otra análoga del interno, será reprimido con pena privativa de libertad no menor de dos ni mayor de cuatro años.
>
> Si el agente se vale de un menor de edad o de su condición de autoridad, abogado defensor, servidor o funcionario público para cometer o permitir que se cometa el hecho

punible descrito, la pena privativa será no menor de tres ni mayor de seis años e inhabilitación, conforme al artículo 36, incisos 1 y 2, del presente Código.

Artículo 368-C. Sabotaje de los equipos de seguridad y de comunicación en establecimientos penitenciarios

El que dentro de un centro de detención o reclusión vulnera, impide, dificulta, inhabilita o de cualquier otra forma imposibilite el funcionamiento de los equipos de seguridad y/o de comunicación en los establecimientos penitenciarios, será reprimido con pena privativa de libertad no menor de cinco ni mayor de ocho años.

Si el agente se vale de un menor de edad o de su condición de autoridad, abogado defensor, servidor o funcionario público para cometer o permitir que se cometa el hecho punible descrito, la pena privativa será no menor de ocho ni mayor de diez años e inhabilitación, conforme al artículo 36, incisos 1 y 2, del presente Código.

Artículo 368-D. Posesión indebida de teléfonos celulares o, armas, municiones o materiales explosivos, inflamables, asfixiantes o tóxicos en establecimientos penitenciarios

La persona privada de libertad en un centro de detención o reclusión, que posea o porte un arma de fuego o arma blanca, municiones o materiales explosivos, inflamables, asfixiantes o tóxicos, será reprimida con pena privativa de libertad no menor de ocho ni mayor de quince años.

Si el agente posee, porta, usa o trafica con un teléfono celular o fijo o cualquiera de sus accesorios que no esté expresamente autorizado, la pena privativa de libertad será no menor de tres ni mayor de ocho años.

Si se demuestra que del ***uso*** de estos aparatos se cometió o intentó cometer un ilícito penal, la pena será no menor de diez ni mayor de quince años.

Delitos contra la fe pública

Artículo 427. Falsificación de documentos

El que hace, en todo o en parte, un documento falso o adultera uno verdadero que pueda dar origen a derecho u obligación o servir para probar un hecho, con el propósito de utilizar el documento, será reprimido, si de su uso puede resultar algún perjuicio, con pena privativa de libertad no menor de dos ni mayor de diez años y con treinta a noventa días-multa si se trata de un documento público, registro público, título auténtico o cualquier otro trasmisible por endoso o al portador y con pena privativa de libertad no menor de dos ni mayor de cuatro años, y con ciento ochenta a trescientos sesenticinco días-multa, si se trata de un documento privado.

El que hace uso de un documento falso o falsificado, como si fuese legítimo, siempre que de su uso pueda resultar algún perjuicio, será reprimido, en su caso, con las mismas penas.

Artículo 428. Falsedad ideológica

El que inserta o hace insertar, en instrumento público, declaraciones falsas concernientes a hechos que deban probarse con el documento, con el objeto de emplearlo como si la declaración fuera conforme a la verdad, será reprimido, si de su uso puede resultar algún perjuicio, con pena privativa de libertad no menor de tres ni mayor de seis años y con ciento ochenta a trescientos sesenticinco días-multa.

El que hace uso del documento como si el contenido fuera exacto, siempre que de su uso pueda resultar algún perjuicio, será reprimido, en su caso, con las mismas penas.

Faltas contra el Patrimonio

Artículo 444-A. Protección de señales satelitales encriptadas

El que reciba una señal de satélite portadora de un programa originariamente codificada, a sabiendas que fue decodificada sin la autorización del distribuidor legal de la señal, será reprimido con cuarenta a ochenta jornadas de prestación de servicios a la comunidad o de diez a sesenta días-multa.

Código Procesal Penal

La Policía

Artículo 68. Atribuciones de la Policía

1. La Policía Nacional en función de investigación, sin perjuicio de lo dispuesto en el artículo anterior y en las normas sobre investigación, bajo la conducción del Fiscal, podrá realizar lo siguiente:

(…)

g) Levantar planos, tomar fotografías, realizar grabaciones en video y demás operaciones técnicas o científicas.

(…)

Las actuaciones Procesales

Artículo 119-A. Audiencia

1. La presencia física del imputado es obligatoria en la audiencia del juicio, conforme al inciso 1) del artículo 356, así como en aquellos actos procesales dispuestos por ley.

2. Excepcionalmente, a pedido del fiscal, del imputado o por disposición del juez, podrá utilizarse el método de videoconferencia en casos que el imputado se encuentre privado de su libertad y su traslado al lugar de la audiencia encuentre dificultades por la distancia o porque exista peligro de fuga.

Artículo 129. Citaciones

1. Las víctimas, testigos, peritos, interpretes y depositarios, podrán ser citados por medio de la Policía o por el personal oficial de la Fiscalía o del órgano jurisdiccional, según las directivas que sobre el particular dicte el órgano de gobierno respectivo.

2. En caso de urgencia podrán ser citados verbalmente, por teléfono, por correo electrónico, fax, telegrama o

cualquier otro medio de comunicación, de lo que se hará constar en autos.

(…)

Comunicación entre Autoridades

Artículo 132. Forma

1. Cuando un acto procesal, una diligencia o una información relacionadas con la causa deban ejecutarse por intermedio de otra autoridad, el Juez o el Fiscal podrán encomendarle su cumplimiento.

2. La comunicación de ejecución precisará la autoridad judicial que lo requiere, su competencia para el caso, el acto concreto, diligencia o información solicitada, con todos los datos necesarios para cumplirla, las normas legales que la posibilitan y el plazo de su cumplimiento. La comunicación podrá realizarse con aplicación de cualquier medio que garantice su autenticidad.

3. En caso de urgencia se utilizará fax, telegrama o correo electrónico y, eventualmente, podrá adelantarse telefónicamente el contenido del requerimiento para que se comience a tramitar la diligencia, sin perjuicio de la remisión posterior del mandamiento escrito.

(…)

6. El órgano de gobierno del Poder Judicial y el Fiscal de la Nación dictarán los reglamentos correspondientes y podrán celebrar convenios con otras instituciones públicas para requerir y compartir información así como establecer sistemas de comunicación por internet entre jueces y fiscales.

Formación del Expediente Fiscal y Judicial

Artículo 134. Contenido del Expediente Fiscal.

1. El Fiscal, con motivo de su actuación procesal, abrirá un expediente para la documentación de las actuaciones de la

investigación. Contendrá la denuncia, el Informe Policial de ser el caso, las diligencias de investigación que hubiera realizado o dispuesto ejecutar, los documentos obtenidos, los dictámenes periciales realizados, las actas y las disposiciones y providencias dictadas, los requerimientos formulados, las resoluciones emitidas por el Juez de la Investigación Preparatoria, así como toda documentación útil a los fines de la investigación.

2. El Fiscal de la Nación reglamentará todo lo relacionado con la formación, custodia, conservación, traslado, recomposición y archivo de las actuaciones del Ministerio Público en su función de investigación del delito. Podrá disponer la utilización de los sistemas tecnológicos que se consideren necesarios para el registro, archivo, copia, transcripción y seguridad del expediente.

Artículo 136 .Contenido del Expediente Judicial

1. Una vez que se dicta el auto de citación a juicio, el Juez Penal ordenará formar el respectivo Expediente Judicial. En este Expediente se anexarán:

(…)

2. El Consejo Ejecutivo del Poder Judicial reglamentará todo lo relacionado con la formación, custodia, conservación, traslado, recomposición y archivo del expediente judicial. Podrá disponer la utilización de los sistemas tecnológicos que se consideren necesarios para el registro, archivo, copia, transcripción y seguridad del expediente.

Testimonio

Artículo 169. Testigos residentes fuera del lugar o en el extranjero

1. Si el testigo no reside en el lugar o cerca de donde debe prestar testimonio, siempre que resulte imposible conseguir su traslado al Despacho judicial, se podrá disponer su

declaración por exhorto. De ser posible, y con preferencia, podrá utilizarse el medio tecnológico más apropiado, como la videoconferencia o filmación de su declaración, a la que podrán asistir o intervenir, según el caso, el Fiscal y los abogados de las partes.

2. Si el testigo se halla en el extranjero se procederá conforme a lo dispuesto por las normas sobre cooperación judicial internacional. En estos casos, de ser posible, se utilizará el método de videoconferencia o el de filmación de la declaración, con intervención -si corresponde- del cónsul o de otro funcionario especialmente habilitado al efecto.

La Prueba Documental

Artículo 187. Traducción, Transcripción y Visualización de documentos

1. Todo documento redactado en idioma distinto del castellano, será traducido por un traductor oficial.

2. Cuando el documento consista en una cinta magnetofónica, el Juez o el Fiscal en la Investigación Preparatoria dispondrá, de ser el caso, su transcripción en un acta, con intervención de las partes.

3. Cuando el documento consista en una cinta de vídeo, el Juez o el Fiscal en la Investigación Preparatoria ordenará su visualización y su transcripción en un acta, con intervención de las partes.

4. Cuando la transcripción de la cinta magnetofónica o cinta de vídeo, por su extensión demande un tiempo considerable, el acta podrá levantarse en el plazo de tres días de realizada la respectiva diligencia, previo traslado de la misma por el plazo de dos días para las observaciones que correspondan. Vencido el plazo sin haberse formulado observaciones, el acta será aprobada inmediatamente; de igual manera, el Juez o el Fiscal resolverán las observaciones formuladas al acta, disponiendo lo conveniente.

Control de Identidad y Videovigilancia

Artículo 207. Presupuestos y Ejecución

1. En las investigaciones por delitos violentos, graves o contra organizaciones delictivas, el Fiscal, por propia iniciativa o a pedido de la Policía, y sin conocimiento del afectado, puede ordenar:

a) Realizar tomas fotográficas y registro de imágenes; y,

b) Utilizar otros medios técnicos especiales determinados con finalidades de observación o para la investigación del lugar de residencia del investigado.

Estos medios técnicos de investigación se dispondrán cuando resulten indispensables para cumplir los fines de esclarecimiento o cuando la investigación resultare menos provechosa o se vería seriamente dificultada por otros medios.

2. Estas medidas podrán dirigirse contra otras personas si, en el supuesto del literal a) del numeral anterior, la averiguación de las circunstancias del hecho investigado se vieran, de otra forma, esencialmente dificultadas o, de no hacerlo, resultaren relevantemente menos provechosas. En el supuesto del literal b) del numeral anterior, se podrá dirigir contra otras personas cuando, en base a determinados hechos, se debe considerar que están en conexión con el investigado o cuando resulte indispensable para cumplir la finalidad de la investigación, sin cuya realización se podría frustrar dicha diligencia o su esclarecimiento pueda verse esencialmente agravado.

3. Se requerirá autorización judicial cuando estos medios técnicos de investigación se realicen en el interior de inmuebles o lugares cerrados.

4. Las medidas previstas en el presente artículo también se pueden llevar a cabo si, por la naturaleza y ámbito de la investigación, se ven irremediablemente afectadas terceras personas.

5. Para su utilización como prueba en el juicio, rige el procedimiento de control previsto para la intervención de comunicaciones.

El Control de Comunicaciones y Documentos Privados

La interceptación e incautación postal

Artículo 226. Autorización

1. Las cartas, pliegos, valores, telegramas y otros objetos de correspondencia o envío postal, en las oficinas o empresas -públicas o privadas- postales o telegráficas, dirigidos al imputado o remitidos por él, aun bajo nombre supuesto, o de aquellos de los cuales por razón de especiales circunstancias, se presumiere emanan de él o de los que él pudiere ser el destinatario, pueden ser objeto, a instancia del Fiscal al Juez de la Investigación Preparatoria, de interceptación, incautación y ulterior apertura.

2. La orden judicial se instará cuando su obtención sea indispensable para el debido esclarecimiento de los hechos investigados. Esta medida, estrictamente reservada y sin conocimiento del afectado, se prolongará por el tiempo estrictamente necesario, el que no será mayor que el período de la investigación.

3. Del mismo modo, se podrá disponer la obtención de copias o respaldos de la correspondencia electrónica dirigida al imputado o emanada de él.

(…)

Artículo 227. Ejecución

1. Recabada la autorización, el Fiscal -por sí o encargando su ejecución a un funcionario de la Fiscalía o un efectivo Policial- realizará inmediatamente la diligencia de interceptación e incautación. Acto seguido examinará externamente la correspondencia o los envíos retenidos, sin abrirlos o tomar conocimiento de su contenido, y retendrá

aquellos que tuvieren relación con el hecho objeto de la investigación. De lo actuado se levantará un acta.

2. La apertura, examen y análisis de la correspondencia y envíos se efectuará en el lugar donde el Fiscal lo considere más conveniente para los fines de la investigación, atendiendo a las circunstancias del caso. El Fiscal leerá la correspondencia o revisará el contenido del envío postal retenido. Si tienen relación con la investigación dispondrá su incautación, dando cuenta al Juez de la Investigación Preparatoria. Por el contrario, si no tuvieren relación con el hecho investigado serán devueltos a su destinatario, directamente o por intermedio de la empresa de comunicaciones. La entrega podrá entenderse también con algún miembro de la familia del destinatario o con su mandatario o representante legal. Cuando solamente una parte tenga relación con el caso, a criterio del fiscal, se dejará copia certificada de aquella parte y se ordenará la entrega a su destinatario o viceversa.

3. En todos los casos previstos en este artículo se redactará el acta correspondiente.

La intervención de comunicaciones y Telecomunicaciones

Artículo 230. Intervención, grabación o registro de comunicaciones telefónicas o de otras formas de comunicación y geolocalización de teléfonos móviles

1. El Fiscal, cuando existan suficientes elementos de convicción para considerar la comisión de un delito sancionado con pena superior a los cuatro años de privación de libertad y la intervención sea absolutamente necesaria para proseguir las investigaciones, podrá solicitar al Juez de la Investigación Preparatoria la intervención y grabación de comunicaciones telefónicas, radiales o de otras formas de comunicación. Rige lo dispuesto en el numeral 4) del artículo 226.

2. La orden judicial puede dirigirse contra el investigado o contra personas de las que cabe estimar fundadamente, en mérito a datos objetivos determinados que reciben o tramitan por cuenta del investigado determinadas comunicaciones, o que el investigado utiliza su comunicación.

3. El requerimiento del Fiscal y, en su caso, la resolución judicial que la autorice, deberá indicar el nombre y dirección del afectado por la medida si se conociera, así como, de ser posible, la identidad del teléfono u otro medio de comunicación o telecomunicación a intervenir, grabar o registrar. También indicará la forma de la interceptación, su alcance y su duración, al igual que la dependencia policial o Fiscalía que se encargará de la diligencia de intervención y grabación o registro.

El Juez comunicará al Fiscal que solicitó la medida el mandato judicial de levantamiento del secreto de las comunicaciones. La comunicación a los concesionarios de servicios públicos de telecomunicaciones, a efectos de cautelar la reserva del caso, será mediante oficio y en dicho documento se transcribirá la parte concerniente.

4. Los concesionarios de servicios públicos de telecomunicaciones deben facilitar, en forma inmediata, la geolocalización de teléfonos móviles y la diligencia de intervención, grabación o registro de las comunicaciones que haya sido dispuesta mediante resolución judicial, en tiempo real y en forma ininterrumpida, las 24 horas de los 365 días del año, bajo apercibimiento de ser pasible de las responsabilidades de Ley en caso de incumplimiento. Los servidores de las indicadas empresas deben guardar secreto acerca de las mismas, salvo que se les citare como testigo al procedimiento.

Dichos concesionarios otorgarán el acceso, la compatibilidad y conexión de su tecnología con el Sistema de Intervención y Control de las Comunicaciones de la Policía Nacional del Perú. Asimismo, cuando por razones

de innovación tecnológica los concesionarios renueven sus equipos y software, se encontrarán obligados a mantener la compatibilidad con el sistema de intervención y control de las comunicaciones de la Policía Nacional del Perú.

5. Si los elementos de convicción tenidos en consideración para ordenar la medida desaparecen o hubiere transcurrido el plazo de duración fijado para la misma, ella deberá ser interrumpida inmediatamente.

6. La interceptación no puede durar más de sesenta días. Excepcionalmente podrá prorrogarse por plazos sucesivos, previo requerimiento sustentado del Fiscal y decisión motivada del Juez de la Investigación Preparatoria."

Artículo 231. Registro de la intervención de comunicaciones telefónicas o de otras formas de comunicación

1. La intervención de comunicaciones telefónicas, radiales o de otras formas de comunicación que trata el artículo anterior será registrada mediante la grabación y aseguramiento de la fidelidad de la misma. Las grabaciones, indicios y/o evidencias recolectadas durante el desarrollo de la ejecución de la medida dispuesta por mandato judicial y el Acta de Recolección y Control serán entregados al Fiscal, quien dispone su conservación con todas las medidas de seguridad al alcance y cuida que las mismas no sean conocidas por personas ajenas al procedimiento.

2. Durante la ejecución del mandato judicial de los actos de recolección y control de las comunicaciones se dejará constancia en el Acta respectiva de dichos actos. Posteriormente, el Fiscal o el Juez podrán disponer la transcripción de las partes relevantes de las comunicaciones, levantándose el acta correspondiente, sin perjuicio de conservar la grabación completa de la comunicación. Las grabaciones serán conservadas hasta la culminación del proceso penal correspondiente, ocasión en la cual la

autoridad judicial competente dispondrá la eliminación de las comunicaciones irrelevantes. Igual procedimiento adoptará el Fiscal en caso la investigación no se judicialice, previa autorización del Juez competente.

Respecto a las grabaciones en las que se aprecie la comisión de presuntos delitos ajenos a los que son materia de la investigación, el Fiscal comunicará estos hechos al Juez que autorizó la medida, con la celeridad e inmediatez que el caso amerita.

Las Actas de Recolección y Control de las Comunicaciones se incorporarán a la investigación, al igual que la grabación de las comunicaciones relevantes."

3. Una vez ejecutada la medida de intervención y realizadas las investigaciones inmediatas en relación al resultado de aquélla, se pondrá en conocimiento del afectado todo lo actuado, quien puede instar el reexamen judicial, dentro del plazo de tres días de notificado. La notificación al afectado sólo será posible si el objeto de la investigación lo permitiere y en tanto no pusiere en peligro la vida o la integridad corporal de terceras personas. El secreto de las mismas requerirá resolución judicial motivada y estará sujeta a un plazo que el Juez fijará.

4. La audiencia judicial de reexamen de la intervención se realizará en el más breve plazo. Estará dirigida a verificar sus resultados y que el afectado haga valer sus derechos y, en su caso, impugnar las decisiones dictadas en ese acto.

5. Si durante la ejecución del mandato judicial de intervención y control de las comunicaciones en tiempo real, a través de nuevos números telefónicos o de identificación de comunicaciones, se tomará conocimiento de la comisión de delitos que atenten contra la vida e integridad de las personas, y cuando se trate de los delitos de terrorismo, tráfico ilícito de drogas y secuestro, a cometerse en las próximas horas, el Fiscal, excepcionalmente y dando

cuenta en forma inmediata al Juez competente para su convalidación, podrá disponer la incorporación de dicho número al procedimiento de intervención de las comunicaciones ya existente, siempre y cuando el Juez en el mandato judicial prevenga esta eventualidad.

Medidas de Protección

Artículo 248. Medidas de protección

1. El Fiscal o el Juez, según el caso, apreciadas las circunstancias previstas en el artículo anterior, de oficio o a instancia de las partes, adoptará según el grado de riesgo o peligro, las medidas necesarias para preservar la identidad del protegido, su domicilio, profesión y lugar de trabajo, sin perjuicio de la acción de contradicción que asista al imputado.

2. Las medidas de protección que pueden adoptarse son las siguientes:

(…)

e) Utilización de cualquier procedimiento que imposibilite su identificación visual normal en las diligencias que se practiquen.

(…)

g) Utilización de procedimientos tecnológicos, tales como videoconferencias u otros adecuados, siempre que se cuenten con los recursos necesarios para su implementación. Esta medida se adoptará para evitar que se ponga en peligro la seguridad del protegido una vez desvelada su identidad y siempre que lo requiera la preservación del derecho de defensa de las partes.

La Detención

Artículo 259. Detención Policial

La Policía Nacional del Perú detiene, sin mandato judicial, a quien sorprenda en flagrante delito. Existe flagrancia cuando:

(…)

3. El agente ha huido y ha sido identificado durante o inmediatamente después de la perpetración del hecho punible, sea por el agraviado o por otra persona que haya presenciado el hecho, o por medio audiovisual, dispositivos o equipos con cuya tecnología se haya registrado su imagen, y es encontrado dentro de las veinticuatro (24) horas de producido el hecho punible.

Artículo 261. Detención Preliminar Judicial

1. El Juez de la Investigación Preparatoria, a solicitud del Fiscal, sin trámite alguno y teniendo a la vista las actuaciones remitidas por aquél, dictará mandato de detención preliminar, cuando:

a) No se presente un supuesto de flagrancia delictiva, pero existan razones plausibles para considerar que una persona ha cometido un delito sancionado con pena privativa de libertad superior a cuatro años y, por las circunstancias del caso, puede desprenderse cierta posibilidad de fuga.

b) El sorprendido en flagrante delito logre evitar su detención.

c) El detenido se fugare de un centro de detención preliminar.

2. En los supuestos anteriores, para cursar la orden de detención se requiere que el imputado se encuentre debidamente individualizado con los siguientes datos: nombres y apellidos completos, edad, sexo, lugar, y fecha de nacimiento.

3. La orden de detención deberá ser puesta en conocimiento de la Policía a la brevedad posible, de manera escrita bajo cargo, quien la ejecutará de inmediato. Cuando se presenten circunstancias extraordinarias podrá ordenarse el cumplimiento de detención por correo electrónico, facsímil, telefónicamente u otro medio de comunicación

válido que garantice la veracidad del mandato judicial. En todos estos casos la comunicación deberá contener los datos de identidad personal del requerido conforme a lo indicado en el numeral dos.

La comparecencia

Artículo 287. Comparecencia restrictiva

(…)

5. También podrá disponerse, alternativamente, la utilización de la vigilancia electrónica personal que permita controlar que no se excedan las restricciones impuestas a la libertad personal, de conformidad a la ley de la materia y su reglamento

Artículo 288. Las restricciones

(…)

5. La vigilancia electrónica personal, de conformidad a la ley de la materia y su reglamento, la que se cumplirá de la siguiente forma:

a) La ejecución se realizará en el domicilio o lugar que señale el imputado, a partir del cual se determinará su radio de acción, itinerario de desplazamiento y tránsito.

b) El imputado estará sujeto a vigilancia electrónica personal para cuyo cumplimiento el juez fijará las reglas de conducta que prevé la ley, así como todas aquellas reglas que consideren necesarias a fin de asegurar la idoneidad del mecanismo de control.

c) El imputado que no haya sido anteriormente sujeto de sentencia condenatoria por delito doloso podrá acceder a la vigilancia electrónica personal. Se dará prioridad a:

i. Los mayores de 65 años.

ii. Los que sufren de enfermedad grave, acreditada con pericia médico legal.

iii. Los que adolezcan de discapacidad física o permanente que afecte sensiblemente su capacidad de desplazamiento.

iv. Las mujeres gestantes dentro del tercer trimestre del proceso de gestación. Igual tratamiento tendrán durante los doce meses siguientes a las fecha de nacimiento.

v. La madre que sea cabeza de familia con hijo menor o con hijo o cónyuge que sufra de discapacidad permanente, siempre y cuando haya estado bajo su cuidado. En ausencia de ella, el padre que se encuentre en las mismas circunstancias tendrá el mismo tratamiento.

d) El imputado deberá previamente acreditar las condiciones de vida personal laboral, familiar y social con un informe social y pericia psicológica.

Artículo 290. Detención domiciliaria

(…)

4. También podrá disponerse la detención domiciliaria del imputado bajo la utilización de la vigilancia electrónica personal, de conformidad a la ley de la materia y su reglamento.

El Juzgamiento

Artículo 357. Publicidad del Juicio y restricciones

1. El juicio oral será público. No obstante ello, el Juzgado mediante auto especialmente motivado podrá resolver, aún de oficio, que el acto oral se realice total o parcialmente en privado, en los siguientes casos:

a) Cuando se afecte directamente el pudor, la vida privada o la integridad física de alguno de los participantes en el juicio;

b) Cuando se afecte gravemente el orden público o la seguridad nacional;

c) Cuando se afecte los intereses de la justicia o, enunciativamente, peligre un secreto particular, comercial o industrial, cuya revelación indebida sea punible o cause perjuicio injustificado,

así como cuando sucedan manifestaciones por parte del público que turben el regular desarrollo de la audiencia;

d) Cuando esté previsto en una norma específica;

2. El Juzgado también podrá disponer, individual o concurrentemente, con sujeción al principio de proporcionalidad, las siguientes medidas:

a) Prohibir el acceso u ordenar la salida de determinadas personas de la Sala de Audiencias cuando afecten el orden y el decoro del juicio;

b) Reducir, en ejercicio de su facultad disciplinaria, el acceso de público a un número determinado de personas, o, por las razones fijadas en el numeral anterior, ordenar su salida para la práctica de pruebas específicas;

c) Prohibir el acceso de cámaras fotográficas o de filmación, grabadoras, o cualquier medio de reproducción mecánica o electrónica de imágenes, sonidos, voces o similares, siempre que considere que su utilización puede perjudicar los intereses de la justicia y, en especial, el derecho de las partes.

Artículo 360. Continuidad, suspensión e interrupción del juicio

1. Instalada la audiencia, ésta seguirá en sesiones continuas e ininterrumpidas hasta su conclusión. Si no fuere posible realizar el debate en un solo día, éste continuará durante los días consecutivos que fueran necesarios hasta su conclusión.

(…)

4. Si en la misma localidad se halla enfermo un testigo o un perito cuyo examen se considera de trascendental importancia, el Juzgado puede suspender la audiencia para constituirse en su domicilio o centro de salud, y examinarlo. A esta declaración concurrirán el Juzgado y las partes. Las declaraciones, en esos casos, se tomarán literalmente, sin perjuicio de filmarse o grabarse. De ser posible, el Juzgado utilizará el método de videoconferencia.

(…)

La actuación probatoria

Artículo 381. Audiencia especial para testigos y peritos

1. Los testigos y peritos que no puedan concurrir a la Sala de Audiencias por un impedimento justificado, serán examinados en el lugar donde se hallen por el juez.

2. Si se encuentran en lugar distinto al del juicio, el juez se trasladará hasta el mismo o empleará el sistema de vídeo conferencia, en el primer supuesto los defensores podrán representar a las partes.

3. En casos excepcionales, el juez comisionará a otro órgano jurisdiccional para la práctica de la prueba, pudiendo intervenir en la misma los abogados de las partes, el acta deberá reproducir íntegramente la prueba y, si se cuenta con los medios técnicos correspondientes, se reproducirá a través de video, filmación o audio.

Extradición

Artículo 521-C. Audiencia ante la Corte Suprema

(….)

2. La Sala Penal escucha a los sujetos procesales, quienes pueden presentar pruebas, cuestionar o apoyar las que aparezcan en el expediente de extradición, alegar la pertinencia o la impertinencia, formal o material, de la demanda de extradición, o cuanto motivo a favor de sus pretensiones. La audiencia se inicia con la precisión de las causales de extradición, el detalle del contenido de la demanda de extradición y la glosa de documentos y elementos de prueba acompañados. Luego el reclamado, si así lo considera conveniente, declara al respecto y se somete al interrogatorio de las partes. A continuación alegan las partes por su orden y, finalmente, el imputado tiene derecho a la última palabra. Concluido el debate,

la Sala Penal se pronuncia declarando procedente o improcedente el pedido de extradición emitiendo su decisión en la misma audiencia. Excepcionalmente, cuando resulte necesario, la Sala puede celebrar audiencias utilizando los medios tecnológicos más apropiados, como la videoconferencia u otros.

(…)

Artículo 523. Detención Preventiva con fines de extradición

(…)

2. La solicitud formal de la detención es remitida a la Fiscalía de la Nación por intermedio de la autoridad central del Estado requirente, o por conducto de la INTERPOL. En casos de urgencia, la solicitud de la detención puede presentarse por cualquier medio, inclusive telegráfico, telefónico, radiográfico o electrónico. La solicitud formal contendrá:

a) El nombre de la persona reclamada, con sus datos de identidad personal y las circunstancias que permitan encontrarla en el país;

b) La fecha, lugar de comisión y tipificación del hecho imputado;

c) Si el requerido fuese un imputado, indicación de la pena conminada para el hecho perpetrado; y, si fuera un condenado, precisión de la pena impuesta;

d) La invocación de la existencia de la orden judicial de detención o de prisión, y de ausencia o contumacia en su caso;

e) El compromiso del Estado solicitante a presentar el pedido formal de extradición.

Código de Ejecución Penal

Artículo 37. Derecho de Comunicación

> El interno puede comunicarse periódicamente, en forma oral y escrita y en su propio idioma, con sus familiares, amigos, representantes diplomáticos y organismos e instituciones de asistencia penitenciaria, salvo la incomunicación declarada por la autoridad judicial en el caso del procesado, conforme a los artículos 140, 141 y 142 del Código Procesal Penal.
>
> Las comunicaciones se realizan respetando la intimidad y privacidad del interno y sus interlocutores.

Semi Libertad y Libertad Condicional

Artículo 53. Procedimiento

> (…)
>
> El juez resolverá en el mismo acto de la audiencia o dentro de los dos días hábiles de celebrada la misma. De otorgar el beneficio, fijará las reglas de conducta que deberá cumplir el beneficiado, pudiendo disponer la utilización de la vigilancia electrónica personal como mecanismo de control.
>
> (…)

Artículo 54. Obligaciones del beneficiado

> (…)
>
> En cualquier caso, el beneficiado se encuentra sujeto a control e inspección del representante del Ministerio Público y de la autoridad penitenciaria. Asimismo, puede estar sujeto a la vigilancia electrónica personal.

Artículo 56. Revocatoria

> Los beneficios penitenciarios de semi-libertad o liberación condicional se revocan si el beneficiado comete un

nuevo delito doloso; incumple las reglas de conducta establecidas en el artículo 55 de la presente norma; o infringe la adecuada utilización y custodia del mecanismo de vigilancia electrónica personal.

Establecimientos Penitenciarios

Artículo 105. Servicios necesarios del establecimiento penitenciario

Los Establecimientos Penitenciarios cuentan con los servicios necesarios, incluyendo ambientes para enfermería, escuela, biblioteca, talleres, instalaciones deportivas y recreativas, locutorios y salas anexas para relaciones familiares y todo aquello que permite desarrollar en los internos una vida en colectividad organizada y una adecuada clasificación en relación con los fines que, en cada caso, les están atribuidos. De acuerdo al régimen penitenciario establecido, la administración penitenciaria establecerá el control del dinero y de las compras de artículos a través de medios electrónicos, coadyuvando a la seguridad penitenciaria.

Ley 27697, Ley que otorga facultad al fiscal para la Intervención y control de comunicaciones y documentos privados en caso excepcional, modificado por Decreto Legislativo 991

Artículo 1. Marco y finalidad

La presente Ley tiene por finalidad desarrollar legislativamente la facultad constitucional otorgada a los jueces para conocer y controlar las comunicaciones de las personas que son materia de investigación preliminar o jurisdiccional.

Solo podrá hacerse uso de la facultad prevista en la presente Ley en los siguientes delitos:

1. Secuestro
2. Trata de personas.
3. Pornografía infantil.
4. Robo agravado.
5. Extorsión.
6. Trafico ilícito de drogas.
7. Trafico ilícito de migrantes.
8. Delitos contra la humanidad.
9. Atentados contra la seguridad nacional o traición a la patria.
10. Peculado.
11. Corrupción de funcionarios.
12. Terrorismo.
13. Delitos tributarios y aduaneros.
14. Lavado de activos.
15. Delitos informáticos.

Ley 30077, Ley contra el crimen organizado

Artículo 3. Delitos comprendidos

La presente Ley es aplicable a los siguientes delitos:

(…)

9. Delitos informáticos, previstos en la ley penal.

(…)

Decreto Legislativo 1182, Decreto que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado.

Artículo 1. Objeto

El presente decreto legislativo tiene por objeto fortalecer las acciones de prevención, investigación y combate de la delincuencia común y el crimen organizado, a través del uso de tecnologías de la información y comunicaciones por parte de la Policía Nacional del Perú.

Artículo 2. Finalidad

La finalidad del presente decreto legislativo es regular el acceso de la unidad especializada de la Policía Nacional del Perú, en casos de flagrancia delictiva, a la localización o geolocalización de teléfonos móviles o dispositivos electrónicos de naturaleza similar.

Artículo 3. Procedencia

La unidad a cargo de la investigación policial solicita a la unidad especializada el acceso inmediato a los datos de localización o geolocalización de teléfonos móviles o dispositivos electrónicos de naturaleza similar, siempre que concurran los siguientes presupuestos:

a. Cuando se trate de flagrante delito, de conformidad con lo dispuesto en el artículo 259 del Decreto Legislativo Nº 957, Código Procesal Penal.

b. Cuando el delito investigado sea sancionado con pena superior a los cuatro años de privación de libertad.

c. El acceso a los datos constituya un medio necesario para la investigación.

Artículo 4. Procedimiento

4.1 La unidad a cargo de la investigación policial, una vez verificados los supuestos del artículo precedente, pone en conocimiento del Ministerio Público el hecho y formula el requerimiento a la unidad especializada de la Policía Nacional del Perú para efectos de la localización o geolocalización.

4.2 La unidad especializada de la Policía Nacional del Perú que recibe el requerimiento, previa verificación del responsable de la unidad solicitante, cursa el pedido a los concesionarios de los servicios públicos de telecomunicaciones o a las entidades públicas relacionadas con estos servicios, a través del correo electrónico institucional u otro medio idóneo convenido.

4.3 Los concesionarios de servicios públicos de telecomunicaciones o las entidades públicas relacionadas con estos servicios, están obligados a brindar los datos de localización o geolocalización de manera inmediata, las veinticuatro (24) horas del día de los trescientos sesenta y cinco (365) días del año, bajo apercibimiento de ser pasible de las responsabilidades de ley en caso de incumplimiento.

4.4 La unidad a cargo de la investigación policial realiza las diligencias pertinentes en consideración a la información obtenida y a otras técnicas de investigación, sin perjuicio de lo establecido en el artículo 5.

Artículo 5. Convalidación Judicial

5.1 La unidad a cargo de la investigación policial, dentro de las 24 horas de comunicado el hecho al Fiscal correspondiente, le remitirá un informe que sustente el requerimiento para su convalidación judicial.

5.2 El Fiscal dentro de las veinticuatro (24) horas de recibido el informe, solicita al Juez la convalidación de la medida.

5.3 El juez competente resolverá mediante trámite reservado y de manera inmediata, teniendo a la vista los recaudos del requerimiento fiscal, en un plazo no mayor de 24 horas. La denegación del requerimiento deja sin efecto la medida y podrá ser apelada por el Fiscal. El recurso ante el juez superior se resolverá en el mismo plazo y sin trámite alguno.

5.4 El juez que convalida la medida establecerá un plazo que no excederá de sesenta (60) días. Excepcionalmente podrá prorrogarse por plazos sucesivos, previo requerimiento sustentado del Fiscal.

Artículo 6. Exclusión y protección del secreto de las telecomunicaciones

El presente decreto legislativo está referido estrictamente a los datos de localización o geolocalización y se excluyen expresamente cualquier tipo de intervención de las telecomunicaciones, las que se rigen por los procedimientos correspondientes.

Artículo 7. Responsabilidades por uso indebido de los datos de localización o geolocalización

7.1 Los denunciantes o el personal policial que realicen actos de simulación de hechos conducentes a la aplicación de la intervención excepcional de la Unidad Especializada de la Policía Nacional del Perú son pasibles de sanción administrativa, civil y penal según corresponda.

7.2 Los que valiéndose de su oficio, posición, jerarquía, autoridad o cargo público induzcan, orienten o interfieran de algún modo en el procedimiento establecido en el Artículo 4, son pasibles de sanción administrativa, civil y penal según corresponda.

7.3 Los concesionarios de servicios públicos de telecomunicaciones o las entidades públicas relacionadas con estos servicios así como los que participan en el proceso de acceso a los datos de localización o geolocalización, están obligados a guardar reserva, bajo responsabilidad administrativa, civil y penal según corresponda.

Artículo 8. Exención de responsabilidad

Los concesionarios de servicios públicos de telecomunicaciones o las entidades públicas relacionadas con estos servicios están exentos de responsabilidad por el suministro de datos de localización o geolocalización, en el marco del presente decreto legislativo.

Artículo 9. Financiamiento

La implementación de las acciones correspondientes al pliego Ministerio del Interior previstas en el presente Decreto Legislativo, se financian con cargo al presupuesto institucional de dicho pliego, sin demandar recursos adicionales al Tesoro Público

Disposiciones Complementarias Finales

Primera. Implementación

Para los efectos de la entrega de los datos de localización o geolocalización de teléfonos móviles o dispositivos electrónicos de naturaleza similar, los concesionarios de servicios públicos de telecomunicaciones y las entidades públicas o privadas relacionadas con estos servicios, implementan mecanismos de acceso exclusivo a la unidad especializada de la Policía Nacional del Perú.

Segunda. Conservación de los datos derivados de las telecomunicaciones

Los concesionarios de servicios públicos de telecomunicaciones y las entidades públicas relacionadas con estos servicios deben conservar los datos derivados de las telecomunicaciones durante los primeros doce (12) meses en sistemas informáticos que permitan su consulta y entrega en línea y en tiempo real. Concluido el referido periodo, deberán conservar dichos datos por veinticuatro (24) meses adicionales, en un sistema de almacenamiento electrónico. La entrega de datos almacenados por un periodo no mayor a doce meses, se realiza en línea y en tiempo real después de recibida la autorización judicial. Para el caso de los datos almacenados por un periodo mayor a doce meses, se hará entrega dentro de los siete (7) días siguientes a la autorización judicial, bajo responsabilidad.

Tercera. Auditoría Operativa

La Inspectoría General del Ministerio del Interior y la Inspectoría General de la Policía Nacional del Perú realizarán auditorías operativas relacionadas con el cumplimiento del presente decreto legislativo.

Cuarta. Contraloría General de la República

La Contraloría General de la República, a través del Órgano de Control Institucional y en el marco del Sistema Nacional de Control, vela por el adecuado cumplimiento de lo dispuesto en el presente decreto legislativo.

Quinta. Mecanismos de advertencia y reporte de datos

Los concesionarios de servicios públicos de telecomunicaciones implementarán mecanismos de advertencia al destinatario de una comunicación producida desde un establecimiento penitenciario o de inmediaciones a este, a través de un mensaje previo

indicando esta circunstancia. Los concesionarios de servicios públicos de telecomunicaciones comunicarán a la unidad especializada el reporte de los datos identificatorios de teléfonos móviles o dispositivos electrónicos de naturaleza similar cuyas llamadas proceden de establecimientos penitenciarios.

Sexta. Infracciones y Sanciones relativas a empresas operadoras

El Ministerio de Transportes y Comunicaciones y el Organismo Regulador de las Telecomunicaciones (OSIPTEL), mediante Decreto Supremo, establecerán las infracciones y sanciones aplicables a los sujetos obligados a brindar acceso a datos derivados de Telecomunicaciones, por el incumplimiento de las obligaciones establecidas en la presente norma y su reglamento.

Disposiciones Complementarias Transitorias

Primera. Plazos para la implementación

En un plazo no mayor de treinta (30) días la unidad especializada de la Policía Nacional del Perú en coordinación con los concesionarios de servicios públicos de telecomunicaciones y con el apoyo técnico de la Dirección Ejecutiva de Tecnología de Información y Comunicaciones de la Policía Nacional del Perú, podrán elaborar protocolos para el mejor acceso de los datos de localización o geolocalización. En un plazo no mayor de treinta (30) días, a partir de la emisión de los citados protocolos, los concesionarios de servicios públicos de telecomunicaciones y las entidades públicas o privadas relacionadas con estos servicios y la unidad especializada con apoyo técnico de la Dirección Ejecutiva de Tecnología de Información y Comunicaciones de la Policía Nacional del Perú diseñarán e implementarán las herramientas tecnológicas necesarias que viabilicen la aplicación de la presente norma.

Segunda. Fortalecimiento de la Unidad Especializada de la Policía Nacional del Perú

El Ministerio del Interior en un plazo no mayor de treinta (30) días, proporcionará los recursos logísticos y económicos, para el fortalecimiento de la unidad especializada de la Policía Nacional del Perú. La Policía Nacional del Perú dotará del personal calificado necesario a la unidad especializada para el mejor cumplimiento de sus funciones e implementará un procedimiento especial de selección que incluirá la entrevista personal, exámenes toxicológicos y psicológicos, así como la prueba del polígrafo. Dicho personal estará sujeto a evaluación permanente. La Dirección Ejecutiva de Educación y Doctrina de la Policía Nacional del Perú establece cursos de capacitación, especialización y perfeccionamiento para el personal de la unidad especializada a la que se refiere el presente decreto legislativo.

Decreto Legislativo 1218, Regula el uso de las cámaras de videovigilancia

Artículo 1. Objeto

El presente decreto legislativo tiene como objeto regular el uso de cámaras de videovigilancia en bienes de dominio público, vehículos de servicio de transporte público de pasajeros y establecimientos comerciales abiertos al público con un aforo de cincuenta (50) personas o más, como instrumento de vigilancia ciudadana, para la prevención de la violencia y del delito, así como el control y persecución del delito o falta en el marco del Sistema Nacional de Seguridad Ciudadana

Artículo 2. Definiciones

Para efectos de la presente norma se tendrán en cuenta las siguientes definiciones:

a. Aforo. Número de personas que puede albergar una edificación determinada en función del uso y de su correspondiente índice dado generalmente en personas/m2.

b. Bienes de dominio público. Aquellos bienes estatales destinados al uso público, cuya administración, conservación y mantenimiento corresponde a una entidad; aquellos que sirven de soporte para la prestación de cualquier servicio público o cuya concesión compete al Estado. Tienen el carácter de inalienables e imprescriptibles. Sobre ellos, el Estado ejerce su potestad administrativa, reglamentaria y de tutela conforme a ley.

c. Cámara o videocámara. Medio técnico análogo, digital, óptico o electrónico, fijo o móvil, que permita captar o grabar imágenes, videos o audios.

d. Establecimientos comerciales abiertos al público. Inmueble, parte del mismo o una instalación o construcción en el que un proveedor debidamente identificado desarrolla

sus actividades económicas de venta de bienes o prestación de servicios a los consumidores.

e. Servicio de transporte público de pasajeros. Servicio de transporte terrestre de personas que es prestado por un transportista autorizado para dicho fin, a cambio de una contraprestación económica. f. Videovigilancia. Sistema de monitoreo y captación de imágenes, videos o audios de lugares, personas u objetos.

Artículo 3. Ámbito de Aplicación

3.1. El presente Decreto Legislativo es de aplicación a personas naturales o jurídicas, públicas o privadas, propietarias o poseedoras de cámaras de videovigilancia ubicadas en bienes de dominio público, vehículos de servicio de transporte público de pasajeros y establecimientos comerciales abiertos al público con un aforo de cincuenta (50) personas o más.

3.2. Se excluyen de la aplicación de la presente norma:

a. Las personas naturales o jurídicas, públicas o privadas, propietarias de cámaras de videovigilancia ubicadas en espacios privados, las mismas que se rigen por la normativa de la materia.

b. Los proyectos de asociación público privado que cuenten con contratos suscritos o que estén incorporados al proceso de promoción de inversión privada a la fecha de la entrada en vigencia de la presente norma.

c. Las cámaras de videovigilancia de la Policía Nacional del Perú y de las Fuerzas Armadas, las cuales se rigen bajo su respectivo marco normativo.

Artículo 4. Reglas

Son reglas para el uso de cámaras de videovigilancia:

a. Disponibilidad. Asegurar que las imágenes, videos o audios se encuentren disponibles siempre que una persona autorizada necesite hacer uso de ellos.

b. Integridad. Las imágenes, videos o audios capturados no deben ser alteradas ni manipuladas.

c. Preservación. Salvaguardar las imágenes, videos o audios captados por las cámaras de videovigilancia que presenten indicios razonables de comisión de un delito o falta.

d. Reserva. Todo funcionario o servidor público que conozca de imágenes, videos o audios captados por las cámaras de videovigilancia está obligado a mantener reserva de su contenido.

Artículo 5. Principios

Son principios para la aplicación de la presente norma y su reglamento:

a. Legalidad. Las personas naturales y jurídicas, públicas y privadas que capten, graben, reproduzcan y utilicen las imágenes, videos o audios de cámaras de videovigilancia actúan de acuerdo a la normatividad vigente.

b. Razonabilidad. El cumplimiento de las obligaciones establecidas en el presente decreto legislativo y su reglamento debe guardar una adecuada proporción entre fines y medios, respondiendo al objeto de la norma.

Artículo 6. Participación ciudadana

Todas las personas naturales y jurídicas, públicas y privadas contribuyen a la seguridad ciudadana mediante el desarrollo de acciones coordinadas entre los sistemas de videovigilancia, para asegurar su protección y convivencia pacífica a través de la prevención, control y erradicación de la violencia, delitos y faltas; así como la utilización pacífica de las vías y espacios públicos.

Capítulo II

Videovigilancia en bienes de dominio público, vehículos de servicio de transporte público de pasajeros y establecimientos comerciales abiertos al público

Artículo 7. Uso de cámaras de videovigilancia en bienes de dominio público

> Las personas naturales o jurídicas, públicas o privadas que administren bienes de dominio público deben instalar cámaras de videovigilancia, bajo los estándares técnicos establecidos en el reglamento del presente Decreto Legislativo, para contribuir a la seguridad ciudadana y articularse con la Policía Nacional del Perú y las Gerencias de Seguridad Ciudadana de las municipalidades o la que hagan sus veces. La instalación de cámaras de videovigilancia debe responder al planeamiento territorial y de desarrollo urbano y rural, así como a los planes distritales de seguridad ciudadana. Las cámaras de videovigilancia son utilizadas en playas, plazas, parques, infraestructura vial, vías férreas, caminos, sedes gubernativas e institucionales, escuelas, hospitales, estadios, bienes afectados en uso a la defensa nacional, establecimientos penitenciarios, espacios culturales, cementerios, puertos, aeropuertos y otros destinados al cumplimiento de los fines de responsabilidad estatal, o cuya concesión compete al Estado.

Artículo 8. Uso de cámaras de videovigilancia en vehículos de servicio de transporte público de pasajeros

> Las personas naturales o jurídicas, públicas o privadas que brindan el servicio de transporte público de pasajeros deben instalar cámaras de videovigilancia en las unidades de transporte, de acuerdo a los lineamientos establecidos en el reglamento del presente Decreto Legislativo.

Artículo 9. Uso de cámaras de videovigilancia en establecimientos comerciales abiertos al público

Los propietarios o poseedores de establecimientos comerciales abiertos al público con un aforo de cincuenta (50) personas o más deben instalar cámaras de videovigilancia acorde con la finalidad de garantizar la seguridad de los consumidores y prevención e investigación del delito. Las cámaras de videovigilancia son utilizadas para seguridad en centros comerciales, tiendas por departamentos, entidades financieras, instituciones educativas o culturales, institutos superiores, universidades, establecimientos de salud, entre otros, con la finalidad de prevenir la comisión de delitos o faltas.

Artículo 10. Limitaciones

Las cámaras de videovigilancia no deben captar o grabar imágenes, videos o audios de espacios que vulneren la privacidad o intimidad de las personas. En el reglamento del presente Decreto Legislativo se detallan las limitaciones.

Artículo 11. Implementación del Sistema de Videovigilancia

Para la implementación del Sistema de videovigilancia se deberán tener en cuenta las siguientes acciones:

a. Instalar y administrar cámaras de videovigilancia en respuesta a los planes distritales de seguridad ciudadana.

b. Integrar los sistemas de videovigilancia con los sistemas de alerta, alarmas, centrales de emergencia, entre otros dispositivos electrónicos o aplicativos que coadyuven en la prevención y lucha contra la seguridad ciudadana.

c. Garantizar la interconexión de cámaras de videovigilancia con las plataformas de videovigilancia, radiocomunicación y telecomunicaciones de los Gobiernos Locales y Regionales, y con el Centro Nacional de Video Vigilancia y Radiocomunicación y Telecomunicaciones para la Seguridad Ciudadana.

d. Realizar un mantenimiento adecuado a las cámaras de videovigilancia, así como renovar el equipamiento.

e. Entre otras acciones reguladas en el reglamento del presente Decreto Legislativo.

Artículo 12. Estándares Técnicos para las cámaras de videovigilancia

El reglamento del presente Decreto Legislativo desarrolla los estándares técnicos para las cámaras de videovigilancia ubicadas en los bienes de dominio público para fortalecer la prevención y coadyuvar en la investigación del delito.

Capítulo III

Obligaciones y Responsabilidades

Artículo 13. Obligaciones en la captación y grabación de imágenes, videos o audios

Todas las personas naturales o jurídicas, entidades públicas o privadas propietarias o poseedoras de cámaras de videovigilancia que capten o graben imágenes, videos o audios deben observar lo siguiente:

a. Cuando aparezcan personas identificables deben observar los principios y disposiciones de la normativa de protección de datos personales.

b. Cualquier persona que por razón del ejercicio de sus funciones dentro de instituciones públicas o privadas, tenga acceso a las grabaciones deberá observar la debida reserva y confidencialidad en relación con las mismas.

Artículo 14. Deber de informar y entregar imágenes, videos o audios

La persona natural o jurídica, privada o pública, propietaria o poseedora de cámaras de videovigilancia que capte o grabe imágenes, videos o audios que presenten indicios razonables de la comisión de un

delito o falta, debe informar y hacer entrega de esta información de manera inmediata a la Policía Nacional del Perú o al Ministerio Público, según corresponda. La Policía Nacional del Perú o el Ministerio Público garantiza la confidencialidad de la identidad de las personas que hacen entrega de esta información.

Artículo 15. Cadena de custodia de imágenes, videos o audios

Las imágenes, videos o audios que contengan información para la investigación de un delito o falta, recibidas por la Policía Nacional del Perú o el Ministerio Público, serán preservadas mediante el procedimiento de cadena de custodia, de acuerdo a la normativa de la materia.

Artículo 16. Responsabilidades

Todo funcionario o servidor público, personal de la Policía Nacional del Perú, del Ministerio Público o del Poder Judicial que use, transfiera, difunda o comercialice las grabaciones de imágenes, videos o audios que presenten indicios razonables de la comisión de un delito o falta, será sancionado administrativamente conforme a la normatividad de la materia, sin perjuicio de las acciones civiles y penales que correspondan.

Artículo 17. Financiamiento

Lo dispuesto en el presente Decreto Legislativo se financia con cargo al presupuesto institucional de las entidades públicas involucradas, sin demandar recursos adicionales al Tesoro Público. El financiamiento de la implementación y/o adecuación a los requisitos establecidos en el presente Decreto Legislativo, respecto de las cámaras de videovigilancia, se realizará de manera progresiva, y sujeto a la disponibilidad presupuestal de las entidades involucradas.

Disposiciones Complementarias Finales

PRIMERA. Reglamentación

En un plazo no mayor a noventa (90) días se aprobará el reglamento del presente Decreto Legislativo con el voto aprobatorio del Consejo de Ministros.

SEGUNDA. Adecuación de Estándares Técnicos de Cámaras de videovigilancia en bienes de dominio público

A partir de la entrada en vigencia del reglamento del presente Decreto Legislativo, toda persona natural o jurídica, pública o privada que administre bienes de dominio público deberá adecuarse a los estándares técnicos definidos en dicho reglamento en un plazo no mayor a cinco (5) años. Los nuevos procesos de adquisición referidos a cámaras de videovigilancia deben cumplir los estándares técnicos.

TERCERA. Cámaras de videovigilancia de establecimientos comerciales abiertos al público

La obligación del uso de cámaras de videovigilancia en establecimientos comerciales abiertos al público será incluida en el Formato de Declaración Jurada a ser presentado por el administrado para el trámite de Licencia de Funcionamiento, siendo materia de fiscalización posterior por parte de los gobiernos locales.

CUARTA. Proyectos de Cableado Menores para Transmisión de Datos

Con el objetivo de permitir una correcta transmisión de datos, dispóngase la aplicación de lo dispuesto en el artículo 2 de la Resolución Ministerial N° 186-2015-MINAM para la autorización de proyectos de instalación de medios de transmisión alámbricos menores a 200 metros.

QUINTA. Acceso de la Policía Nacional del Perú a Sistemas de Cámaras y otros sistemas de videovigilancia

> Las Unidades Especializadas de la Policía Nacional del Perú pueden acceder a los sistemas de cámaras de circuito cerrado de televisión (CCTV) y otros sistemas de videovigilancia instalados en puertos, aeropuertos, terminales terrestres, almacenes aduaneros y depósitos temporales que coadyuven al ejercicio de su función.

Disposición Complementaria Modificatoria

ÚNICA.-Incorporación de Infracción al Anexo III, Tabla de Infracciones y Sanciones Muy graves del Decreto Legislativo N°1150, que regula el Régimen Disciplinario de la Policía Nacional del Perú

> Incorpórase la infracción MG 50-B en el Anexo III, Tabla de Infracciones y Sanciones Muy Graves del Decreto Legislativo N°1150, que regula el Régimen Disciplinario de la Policía Nacional del Perú en los términos siguientes:
>
> Código: MG 50- B
>
> Infracción: Usar, transferir, difundir o comercializar las grabaciones de imágenes, videos o audios que constituyen indicio o medio probatorio en una investigación.
>
> Sanción: Pase a la situación de retiro

Ley 30618, Ley que modifica el DL 1141, DL de fortalecimiento y modernización del Sistema de Inteligencia Nacional – SINA y de la Dirección Nacional de Inteligencia, DINI, a fin de regular la seguridad digital

Artículo único. Modificación de los artículos 2, 8, 10, 17 y 38, e incorporación de la disposición complementaria final octava del Decreto Legislativo 1141, Decreto Legislativo de fortalecimiento y modernización del Sistema de Inteligencia Nacional - SINA y de la Dirección Nacional de Inteligencia - DINI

Incorpóranse los numerales 8 al artículo 2 y 8.3 al artículo 8; modifícanse el numeral 10.1 del artículo 10 y los numerales 17.8, 17.13, 17.16, 17.17 del artículo 17; asimismo incorpóranse los numerales 17.18, 17.19 y 17.20 a este mismo artículo 17; modifícase el numeral 38.1 del artículo 38; e incorpórase la disposición complementaria final octava al Decreto Legislativo 1141, Decreto Legislativo de Fortalecimiento y Modernización del Sistema de Inteligencia Nacional - SINA y de la Dirección Nacional de Inteligencia - DINI, modificado por la Ley 30535, en los siguientes términos:

"Artículo 2. Definiciones

Para los fines del presente Decreto Legislativo y de las actividades reguladas por el mismo, se entenderá por:

(…)

8) Seguridad Digital: Es la situación de confianza en el entorno digital, frente a las amenazas que afectan las capacidades nacionales, a través de la gestión de riesgos y la aplicación de medidas de ciberseguridad y las capacidades de ciberdefensa, alineada al logro de los objetivos del Estado.

Artículo 8. Objetivos

El Sistema de Inteligencia Nacional - SINA tiene los siguientes objetivos:

(…)

8.3 Realizar actividades destinadas a alcanzar la seguridad digital en materia de seguridad nacional.

Artículo 10. Plan de Inteligencia Nacional - PIN

10.1 Para efectos del desarrollo de actividades de inteligencia, contrainteligencia y seguridad digital, en el ámbito de su competencia, el Sistema de Inteligencia Nacional - SINA cuenta con el Plan de Inteligencia Nacional - PIN, que contiene los objetivos, políticas, estrategias, gestión de riesgos y responsabilidades de sus componentes, relacionados con las amenazas a la seguridad nacional y la identificación de oportunidades favorables a ella, siendo su cumplimiento de carácter obligatorio. Es aprobado por el Consejo de Seguridad y Defensa Nacional en abril del año anterior a su ejecución, a propuesta del ente rector del Sistema de Inteligencia Nacional - SINA, previa conformidad del Consejo de Inteligencia Nacional - COIN.

Artículo 17. Funciones

Son funciones de la Dirección Nacional de Inteligencia - DINI:

(…)

17.8 Constituir la autoridad técnica normativa a nivel nacional en materia de inteligencia, contrainteligencia y seguridad digital, en el ámbito de su competencia.

(…)

17.13 Establecer y fortalecer las relaciones de cooperación y asistencia con organismos de inteligencia de otros países.

(…)

17.16 En el ámbito de su competencia y de conformidad con la ley de la materia, aprobar y supervisar los programas académicos de formación laboral y profesional, capacitación y perfeccionamiento en materia de inteligencia que se brinden a través de la Escuela Nacional

de Inteligencia - ENI, con la finalidad de asegurar una formación integral y de calidad del personal del Sistema de Inteligencia Nacional - SINA, sustentada en principios y valores democráticos. Asimismo, brindar capacitación y formación laboral y profesional al personal del Sistema de Inteligencia Nacional - SINA, a través de la Escuela Nacional de Inteligencia - ENI o mediante suscripción de convenios de cooperación interinstitucional con universidades, institutos tecnológicos y centros de formación de las Fuerzas Armadas y Policía Nacional del Perú y de otros países.

17.17 Realizar actividades y establecer los procedimientos destinados a alcanzar la seguridad digital en el ámbito de su competencia, en concordancia con los principios y objetivos de la actividad de inteligencia establecidos en el presente decreto legislativo. En el caso de amenazas que afectan o que potencialmente afecten las capacidades nacionales, las entidades públicas y privadas se sujetan a dichos procedimientos.

17.18 Establecer los procedimientos especiales para la obtención de información en entornos digitales a que se refiere el artículo 32 del presente decreto legislativo y para peritajes informáticos. El Poder Judicial, a través de convenios interinstitucionales brinda asesoramiento técnico para la elaboración de estos procedimientos.

17.19 Suscribir convenios interinstitucionales, en el ámbito de su competencia, a nivel nacional o internacional, así como disponer su modificación, ampliación o resolución en materia de inteligencia, contrainteligencia y seguridad digital.

17.20 Las demás establecidas por ley.

Artículo 38. Protección de la identidad

38.1 Los procedimientos de protección de identidad del personal y de la actividad de inteligencia, incluyendo los que se encuentran en entornos digitales, tienen carácter secreto.

(…)

DISPOSICIONES COMPLEMENTARIAS FINALES

(…)

OCTAVA. Elaboración del componente de Seguridad Digital del Plan de Inteligencia Nacional - PIN

La Dirección Nacional de Inteligencia - DINI en coordinación con las entidades nacionales correspondientes elabora el componente de Seguridad Digital del Plan de Inteligencia Nacional - PIN".

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA. Adecuación del Reglamento del Decreto Legislativo 1141

El Poder Ejecutivo adecúa el Reglamento del Decreto Legislativo 1141, Decreto Legislativo de fortalecimiento y modernización del Sistema de Inteligencia Nacional - SINA y de la Dirección Nacional de Inteligencia - DINI, aprobado mediante el Decreto Supremo 016-2014-PCM, a las modificaciones y definiciones establecidas en la presente ley, en el plazo de noventa días calendario siguientes a su entrada en vigencia.

SEGUNDA. Definición de seguridad digital en el ámbito nacional

La Presidencia del Consejo de Ministros, mediante decreto supremo, desarrollará la definición de seguridad digital en el ámbito nacional.

DS 050-2018-PCM: Aprueban la definición de Seguridad Digital en el Ámbito Nacional

Artículo 1. Objeto

El presente decreto supremo tiene por objeto establecer la definición de Seguridad Digital de ámbito nacional, en cumplimiento con la Segunda Disposición Complementaria Final de la Ley N° 30618, Ley que modifica el Decreto Legislativo N° 1141.

Artículo 2. Definición de Seguridad Digital en el ámbito nacional

La Seguridad Digital en el ámbito nacional es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas; debiéndose tener presente para estos efectos los aspectos siguientes:

a) Nota 1: La confianza en el entorno digital o también denominada confianza digital emerge como resultado de cuan veraz, predecible, seguro y confiable son las interacciones digitales que se generan entre empresas, individuos o cosas.

b) Nota 2: Las medidas proactivas y reactivas comprenden tecnología, políticas, controles, programas de capacitación y sensibilización que tienen por finalidad preservar la confidencialidad, integridad y disponibilidad de la información contenida en el entorno digital.

c) Nota 3: Los riesgos en el entorno digital o riesgo de seguridad digital es resultado de una combinación de amenazas y vulnerabilidades en el entorno digital. La gestión del riesgo de seguridad digital comprende los

procesos que garantizan que las acciones o medidas son apropiadas con los riesgos y objetivos económicos y sociales en juego.

d) Nota 4: La prosperidad económica y social comprende la creación de riqueza, la innovación, la competitividad, entre otros, así como aspectos vinculados con las libertades individuales, salud, educación, cultura, participación democrática, ciencia, ocio y otras dimensiones del bienestar en las que el entorno digital está impulsando el progreso.

Artículo 3. Alcance

El presente Decreto Supremo es de alcance obligatorio a todas las entidades de la Administración Pública comprendidas en el Artículo I del Título Preliminar del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 006-2017-JUS.

Artículo 4. Lineamientos de Seguridad Digital

La Secretaría de Gobierno Digital (SEGDI) de la Presidencia del Consejo de Ministros, como órgano rector del Sistema Nacional de Informática, y en coordinación con los actores competentes, dicta las políticas o lineamientos de Seguridad Digital de los sistemas informáticos de las entidades de la administración pública.

Artículo 5. Publicación

El presente Decreto Supremo es publicado en el Diario Oficial "El Peruano", en el Portal del Estado Peruano (www.peru.gob.pe), y en el Portal Institucional de la Presidencia del Consejo de Ministros (www.pcm.gob.pe).

Artículo 6. Refrendo

El presente Decreto Supremo es refrendado por el Presidente del Consejo de Ministros.

DL 1412, Ley de Gobierno Digital

Artículo 1. Objeto

La presente Ley tiene por objeto establecer el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno.

Artículo 2. Ámbito de aplicación

2.1. La presente Ley es de aplicación a toda entidad que forma parte de la Administración Pública a que se refiere el artículo I del Título Preliminar del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General. Sus regulaciones también alcanzan a las personas jurídicas o naturales que, por mandato legal, encargo o relación contractual ejercen potestades administrativas, y por tanto su accionar se encuentra sujeto a normas de derecho público, en los términos dispuestos por la Presidencia del Consejo de Ministros.

2.2. En el caso de las empresas que conforman la actividad empresarial del Estado, su aplicación se da en todo aquello que le resulte aplicable.

Artículo 3. Definiciones

Para efectos de la presente Ley, se adoptan las siguientes definiciones:

1. Tecnologías Digitales. Se refieren a las Tecnologías de la Información y la Comunicación - TIC, incluidos Internet, las tecnologías y dispositivos móviles, así como la analítica de datos utilizados para mejorar la generación, recopilación, intercambio, agregación, combinación,

análisis, acceso, búsqueda y presentación de contenido digital, incluido el desarrollo de servicios y aplicaciones aplicables a la materia de gobierno digital.

2. Entorno Digital. Es el dominio o ámbito habilitado por las tecnologías y dispositivos digitales, generalmente interconectados a través de redes de datos o comunicación, incluyendo el Internet, que soportan los procesos, servicios, infraestructuras y la interacción entre personas.

3. Servicio Digital. Es aquel provisto de forma total o parcial a través de Internet u otra red equivalente, que se caracteriza por ser automático, no presencial y utilizar de manera intensiva las tecnologías digitales, para la producción y acceso a datos y contenidos que generen valor público para los ciudadanos y personas en general.

4. Canal Digital. Es el medio de contacto digital que disponen las entidades de la Administración Pública a los ciudadanos y personas en general para facilitar el acceso a toda la información institucional y de trámites, realizar y hacer seguimiento a servicios digitales, entre otros. Este canal puede comprender páginas y sitios web, redes sociales, mensajería electrónica, aplicaciones móviles u otros.

5. Ciudadano Digital. Es aquel que hace uso de las tecnologías digitales y ejerce sus deberes y derechos en un entorno digital seguro.

6. Gobernanza Digital. Es el conjunto de procesos, estructuras, herramientas y normas que nos permiten dirigir, evaluar y supervisar el uso y adopción de las tecnologías digitales en la organización.

7. Arquitectura Digital. Es el conjunto de componentes, lineamientos y estándares, que desde una perspectiva integral de la organización permiten alinear los sistemas

de información, datos, seguridad e infraestructura tecnológica con la misión y objetivos estratégicos de la entidad, de tal manera que se promuevan la colaboración, interoperabilidad, escalabilidad, seguridad y el uso optimizado de las tecnologías digitales en un entorno de gobierno digital.

Artículo 4. Finalidad

La presente Ley tiene por finalidad:

4.1 Mejorar la prestación y acceso de servicios digitales en condiciones interoperables, seguras, disponibles, escalables, ágiles, accesibles, y que faciliten la transparencia para el ciudadano y personas en general.

4.2 Promover la colaboración entre las entidades de la Administración Pública, así como la participación de ciudadanos y otros interesados para el desarrollo del gobierno digital y sociedad del conocimiento.

Artículo 5. Principios rectores

Las disposiciones contenidas en la presente Ley, así como su aplicación se rigen por los siguientes principios rectores:

5.1 Especialidad. La presente norma es aplicable a los servicios digitales prestados por las entidades de la Administración Pública en un entorno de gobierno digital, sin perjuicio de lo regulado para los procedimientos administrativos u otros que se rigen por su propia normatividad.

5.2 Equivalencia Funcional. El ejercicio de la identidad digital para el uso y prestación de servicios digitales confiere y reconoce a las personas las mismas garantías que otorgan los modos tradicionales de relacionarse entre privados y/o en la relación con las entidades de la Administración Pública.

5.3 Privacidad desde el Diseño. En el diseño y configuración de los servicios digitales se adoptan las medidas preventivas de tipo tecnológico, organizacional, humano y procedimental.

5.4 Igualdad de Responsabilidades. Las entidades de la Administración Pública responden por los actos realizados a través de canales digitales de la misma manera y con iguales responsabilidades que por los realizados a través de medios presenciales.

5.5 Usabilidad. En el diseño y configuración de los servicios digitales se propenderá a que su uso resulte de fácil manejo para los ciudadanos y personas en general.

5.6 Cooperación Digital. Prima el intercambio de datos e información, la interoperabilidad de los sistemas y soluciones para la prestación conjunta de servicios digitales.

5.7 Digital desde el Diseño. Los servicios, de manera preferente, progresiva y cuando corresponda, se diseñan y modelan para que sean digitales de principio a fin.

5.8 Proporcionalidad. Los requerimientos de seguridad y autenticación de los servicios digitales prestados por las entidades de la Administración Pública deben ser proporcionales al nivel de riesgo asumido en la prestación del mismo.

5.9 Datos Abiertos por Defecto. Los datos se encuentran abiertos y disponibles de manera inmediata, sin comprometer el derecho a la protección de los datos personales de los ciudadanos. Ante la duda corresponde a la Autoridad de Transparencia definirlo.

5.10 Nivel de protección adecuado para los datos personales. El tratamiento de los datos personales debe realizarse conforme a lo establecido en la Ley de Protección de Datos Personales y su Reglamento.

TÍTULO II

GOBIERNO DIGITAL

CAPÍTULO I

GOBIERNO DIGITAL

Artículo 6. Gobierno Digital

6.1. El gobierno digital es el uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público. Se sustenta en un ecosistema compuesto por actores del sector público, ciudadanos y otros interesados, quienes apoyan en la implementación de iniciativas y acciones de diseño, creación de servicios digitales y contenidos, asegurando el pleno respeto de los derechos de los ciudadanos y personas en general en el entorno digital.

6.2. Comprende el conjunto de principios, políticas, normas, procedimientos, técnicas e instrumentos utilizados por las entidades de la Administración Pública en la gobernanza, gestión e implementación de tecnologías digitales para la digitalización de procesos, datos, contenidos y servicios digitales de valor para los ciudadanos.

Artículo 7. Objetivos del Gobierno Digital

Los objetivos del gobierno digital son:

7.1 Normar las actividades de gobernanza, gestión e implementación en materia de tecnologías digitales, identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos.

7.2 Coordinar, integrar y promover la colaboración entre las entidades de la Administración Pública.

7.3 Promover la investigación y desarrollo en la implementación de tecnologías digitales, identidad digital, servicios digitales, interoperabilidad, seguridad digital y datos.

7.4 Promover y orientar la formación y capacitación en materia de gobierno digital y tecnologías digitales en todos los niveles de gobierno.

Artículo 8. Ente Rector en materia de Gobierno Digital

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el ente rector en materia de gobierno digital que comprende tecnologías digitales, identidad digital, interoperabilidad, servicio digital, datos, seguridad digital y arquitectura digital. Dicta las normas y establece los procedimientos en materia de gobierno digital y, es responsable de su operación y correcto funcionamiento.

Artículo 9. Funciones del ente rector en materia de gobierno digital

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, en su calidad de ente rector tiene las siguientes atribuciones:

9.1 Programar, dirigir, coordinar, supervisar y evaluar la aplicación de la materia de gobierno digital.

9.2 Elaborar y proponer normas reglamentarias y complementarias que regulan la materia de gobierno digital.

9.3 Elaborar lineamientos, procedimientos, metodologías, modelos, directivas u otros estándares de obligatorio cumplimiento para la implementación de las materias de gobierno digital.

9.4 Emitir opinión vinculante sobre el alcance, interpretación e integración de normas que regulan la materia de gobierno digital.

9.5 Emitir opinión previa a fin de validar técnicamente proyectos de tecnologías digitales de carácter transversal en materia de interoperabilidad, seguridad digital, identidad digital, datos, arquitectura digital o aquellos destinados a mejorar la prestación de servicios digitales.

9.6 Brindar apoyo técnico a las entidades públicas en la gestión e implementación de tecnologías digitales.

9.7 Definir los alcances del marco normativo en materia de gobierno digital.

9.8 Supervisar y fiscalizar, cuando corresponda, el cumplimiento del marco normativo en materia de gobierno digital.

9.9 Promover mecanismos que aseguren la identidad digital como pilar fundamental para la inclusión digital y la ciudadanía digital.

9.10 Promover y gestionar la implementación de proyectos de implementación de tecnologías digitales u otros mecanismos destinados a mejorar la prestación de servicios digitales, en coordinación con las entidades públicas, según corresponda.

9.11 Promover la digitalización de los procesos y servicios a partir del uso e implementación de tecnologías digitales.

9.12 Realizar acciones de coordinación y articulación con representantes de la administración pública, ciudadanos u otros interesados con la finalidad de optimizar el uso de tecnologías digitales para el desarrollo del gobierno digital y tecnologías digitales.

CAPÍTULO II

IDENTIDAD DIGITAL

Artículo 10. De la Identidad Digital

10.1 La identidad digital es aquel conjunto de atributos que individualiza y permite identificar a una persona en entornos digitales.

10.2 Los atributos de la identidad digital son otorgados por distintas entidades de la Administración Pública que, en su conjunto, caracterizan al individuo.

Artículo 11. Marco de Identidad Digital del Estado Peruano

El Marco de Identidad Digital del Estado Peruano está constituido por lineamientos, especificaciones, guías, directivas, estándares e infraestructura de tecnologías digitales, que permiten de manera efectiva la identificación y autenticación de los ciudadanos y personas en general cuando acceden a los servicios digitales.

Artículo 12. Credencial de Identidad Digital

Es la representación de una identidad digital que comprende los atributos inherentes a la persona definidos en el Marco de Identidad Digital del Estado Peruano, a fin de facilitar la autenticación digital.

Artículo 13. Identificación Digital

La identificación digital es el procedimiento de reconocimiento de una persona como distinta de otras, en el entorno digital. Las entidades de la Administración Pública deben establecer los procedimientos para identificar a las personas que accedan a los servicios digitales.

Artículo 14. Autenticación Digital

La autenticación digital es el procedimiento de verificación de la identidad digital de una persona, mediante el cual se puede afirmar que es quien dice ser.

Para el acceso a un servicio digital las entidades de la Administración Pública deben adoptar los mecanismos o procedimientos de autenticación digital, considerando los niveles de seguridad a establecerse en la norma reglamentaria.

Artículo 15. Inclusión digital

La inclusión digital es el acceso y uso de los servicios digitales por parte de los ciudadanos a través de su identidad digital, promoviendo la ciudadanía digital. Para tal fin las entidades

de la Administración Pública adoptan las disposiciones que emite el ente rector para la prestación de dichos servicios.

Artículo 16. Documento Nacional de Identidad electrónico (DNIe)

El Documento Nacional de Identidad Electrónico (DNIe) es una credencial de identidad digital, emitida por el Registro Nacional de Identificación y Estado Civil - RENIEC, que acredita presencial y no presencialmente la identidad de las personas.

Artículo 17. Uso del Documento Nacional de Identidad electrónico

Los funcionarios y servidores públicos al servicio de las entidades de la Administración Pública pueden hacer uso del Documento Nacional de Identidad Electrónico (DNIe) para el ejercicio de sus funciones en los actos de administración, actos administrativos, procedimientos administrativos y servicios digitales.

El DNIe sólo otorga garantía sobre la identificación de la persona natural, mas no en el cargo, rol, atribuciones o facultades que ostenta un funcionario o servidor de una entidad de la Administración Pública; dicho funcionario o servidor público es el responsable de gestionar en su entidad las autorizaciones de acceso y asignación de roles, atribuciones o facultades para hacer uso del indicado DNIe en los sistemas de información que hagan uso del mismo.

CAPÍTULO III

PRESTACIÓN DE SERVICIOS DIGITALES

Artículo 18. Garantías para la prestación de servicios digitales

Las entidades de la Administración Pública, de manera progresiva y cuando corresponda, deben garantizar a las personas el establecimiento y la prestación de los servicios digitales, comprendidos en el ámbito de aplicación de la presente Ley, debiendo para tal efecto:

18.1 Reconocer y aceptar el uso de la identidad digital de todas las personas según lo regulado en la presente Ley.

18.2 Garantizar la disponibilidad, integridad y confidencialidad de la información de los servicios digitales con la aplicación de los controles de seguridad que correspondan en la prestación de dichos servicios conforme a las disposiciones contenidas en la presente Ley y en la normatividad vigente sobre la materia.

18.3 Capacitar en temas en materia de firmas electrónicas, firmas y certificados digitales, protección de datos personales, interoperabilidad, arquitectura digital, seguridad digital, datos abiertos y gobierno digital.

18.4 Facilitar el acceso a la información requerida por otra entidad de la Administración Pública, sobre los datos de las personas que obren en su poder y se encuentren en soporte electrónico, únicamente para el ejercicio de sus funciones en el ámbito de sus competencias. Queda excluida del intercambio la información que pueda afectar la seguridad nacional o aquella relacionada con la legislación sobre Transparencia y Acceso a la Información Pública, o la que expresamente sea excluida por Ley.

18.5 Implementar servicios digitales haciendo un análisis de la arquitectura digital y rediseño funcional.

18.6 Considerar la implementación de pagos a través de canales digitales.

18.7 Facilitar a las personas información detallada, concisa y entendible sobre las condiciones de tratamiento de sus datos personales.

18.8 Garantizar la conservación de las comunicaciones y documentos generados a través de canales digitales en las mismas o mejores condiciones que aquellas utilizadas por los medios tradicionales.

18.9 Garantizar que en el diseño y configuración de los servicios digitales se adoptan las medidas técnicas,

organizativas y legales para la debida protección de datos personales y la confidencialidad de las comunicaciones.

Artículo 19. Conservación de los documentos electrónicos firmados digitalmente

Para conservar documentos electrónicos y garantizar la perdurabilidad en el tiempo de la firma digital incorporada en aquellos se emplean sellos de tiempo y mecanismos basados en estándares internacionalmente aceptados que permitan verificar el estado del certificado digital asociado.

Cuando dicho tipo de documentos electrónicos, y sus respectivos formatos que aseguran la característica de perdurabilidad de la firma digital, deban ser conservados de modo permanente, éstos se archivarán observando las disposiciones legales sobre la materia.

Artículo 20. Sede Digital

La sede digital es un tipo de canal digital, a través del cual pueden acceder los ciudadanos y personas en general a un catálogo de servicios digitales, realizar trámites, hacer seguimiento de los mismos, recepcionar y enviar documentos electrónicos, y cuya titularidad, gestión y administración corresponde a cada entidad de la Administración Pública en los tres niveles de gobierno.

Artículo 21. Registro Digital

Las sedes digitales de las entidades de la Administración Pública cuentan con un registro digital para recibir documentos, solicitudes, escritos y comunicaciones electrónicas dirigidas a dicha entidad.

Artículo 22. Domicilio Digital

Es uno de los atributos de la identidad digital que se constituye en el domicilio habitual de un ciudadano en el entorno digital, el cual es utilizado por las entidades de

la Administración Pública para efectuar comunicaciones o notificaciones.

CAPÍTULO IV

GOBERNANZA DE DATOS

Artículo 23. Datos

23.1 Los datos son la representación dimensionada y descifrable de hechos, información o concepto, expresada en cualquier forma apropiada para su procesamiento, almacenamiento, comunicación e interpretación.

23.2 Las entidades de la Administración Pública administran sus datos como un activo estratégico, garantizando que estos se recopilen, procesen, publiquen, almacenen y pongan a disposición durante el tiempo que sea necesario y cuando sea apropiado, considerando las necesidades de información, riesgos y la normatividad vigente en materia de gobierno digital, seguridad digital, transparencia, protección de datos personales y cualquier otra vinculante.

Artículo 24. Infraestructura Nacional de Datos

La Infraestructura Nacional de Datos se define como el conjunto articulado de políticas, normas, medidas, procesos, tecnologías digitales, repositorios y bases de datos destinadas a promover la adecuada recopilación, procesamiento, publicación, almacenamiento y puesta a disposición de los datos que gestionan las entidades de la Administración Pública.

Artículo 25. Marco de Gobernanza y Gestión de Datos del Estado Peruano

El Marco de Gobernanza y Gestión de Datos del Estado Peruano está constituido por instrumentos técnicos y normativos que establecen los requisitos mínimos que las entidades de la Administración Pública deben implementar conforme a su contexto legal, tecnológico y estratégico para

asegurar un nivel básico y aceptable para la recopilación, procesamiento, publicación, almacenamiento y apertura de los datos que administre.

CAPÍTULO V

INTEROPERABILIDAD

Artículo 26. Interoperabilidad

La Interoperabilidad es la capacidad de interactuar que tienen las organizaciones diversas y dispares para alcanzar objetivos que hayan acordado conjuntamente, recurriendo a la puesta en común de información y conocimientos, a través de los procesos y el intercambio de datos entre sus respectivos sistemas de información.

Artículo 27. Marco de Interoperabilidad del Estado Peruano

El Marco de Interoperabilidad del Estado Peruano está constituido por políticas, lineamientos, especificaciones, estándares e infraestructura de tecnologías digitales, que permiten de manera efectiva la colaboración entre entidades de la Administración Pública para el intercambio de información y conocimiento, para el ejercicio de sus funciones en el ámbito de sus competencias, en la prestación de servicios digitales inter-administrativos de valor para el ciudadano provisto a través de canales digitales.

Artículo 28. Gestión del Marco de Interoperabilidad del Estado Peruano

El Marco de Interoperabilidad del Estado Peruano se gestiona a través de los siguientes niveles:

28.1. Interoperabilidad a nivel organizacional: Se ocupa del alineamiento de objetivos, procesos, responsabilidades y relaciones entre las entidades de la Administración Pública para intercambiar datos e información para el ejercicio de sus funciones en el ámbito de sus competencias.

28.2 Interoperabilidad a nivel semántico: Se ocupa del uso de los datos y la información de una entidad garantizando que el formato y significado preciso de dichos datos e información a ser intercambiada pueda ser entendido por cualquier aplicación de otra entidad de la Administración Pública. Dichas entidades deben adoptar los estándares definidos por el ente rector para el intercambio de datos e información.

28.3. Interoperabilidad a nivel técnico: Se ocupa de los aspectos técnicos relacionados con las interfaces, la interconexión, integración, intercambio y presentación de datos e información, así como definir los protocolos de comunicación y seguridad. Es ejecutado por personal de las Oficinas de Informática o las que hagan sus veces de las entidades de la Administración Pública, de acuerdo con los estándares definidos por el ente rector.

28.4. Interoperabilidad a nivel legal: Se ocupa de la adecuada observancia de la legislación y lineamientos técnicos con la finalidad de facilitar el intercambio de datos e información entre las diferentes entidades de la Administración Pública, así como el cumplimiento de los temas concernientes con el tratamiento de la información que se intercambia.

Artículo 29. Reutilización de Software

Las entidades de la Administración Pública titulares de Software Público Peruano, desarrollado mediante la contratación de terceros o por personal de la entidad para soportar sus procesos o servicios, adoptan las medidas necesarias a fin de obtener la titularidad exclusiva sobre los derechos patrimoniales del referido Software Público Peruano.

Todas las entidades de la Administración Pública deben compartir Software Público Peruano bajo licencias libres o abiertas que permitan (i) usarlo o

ejecutarlo, (ii) copiarlo o reproducirlo, (iii) acceder al código fuente, código objeto, documentación técnica y manuales de uso, (iv) modificarlo o transformarlo en forma colaborativa, y (v) distribuirlo, en beneficio del Estado Peruano.

CAPÍTULO VI

SEGURIDAD DIGITAL

Artículo 30. De la Seguridad Digital

La seguridad digital es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas.

Artículo 31. Marco de Seguridad Digital del Estado Peruano

El Marco de Seguridad Digital del Estado Peruano se constituye en el conjunto de principios, modelos, políticas, normas, procesos, roles, tecnología y estándares mínimos que permitan preservar la confidencialidad, integridad, disponibilidad de la información en el entorno digital administrado por las entidades de la Administración Pública.

Artículo 32. Gestión del Marco de Seguridad Digital del Estado Peruano

El Marco de Seguridad Digital del Estado Peruano tiene los siguientes ámbitos:

a. El Ministerio de Defensa (MINDEF), en el marco de sus funciones y competencias, dirige, norma, supervisa y evalúa las normas en materia de ciberdefensa.

[Modificado por la Ley de Ciberdefensa]

b. Inteligencia: La Dirección Nacional de Inteligencia (DINI) como autoridad técnica normativa en el marco de sus funciones emite, supervisa y evalúa las normas en materia de inteligencia, contrainteligencia y seguridad digital en el ámbito de esta competencia.

c. Justicia: El Ministerio de Justicia y Derechos Humanos (MINJUS), el Ministerio del Interior (MININTER), la Policía Nacional del Perú (PNP), el Ministerio Público y el Poder Judicial (PJ) en el marco de sus funciones y competencias dirigen, supervisan y evalúan las normas en materia de ciberdelincuencia.

d. Institucional: Las entidades de la Administración Pública deben establecer, mantener y documentar un Sistema de Gestión de la Seguridad de la Información (SGSI).

Artículo 33. Articulación de la Seguridad Digital con la Seguridad de la Información

El Marco de Seguridad Digital del Estado Peruano se articula y sustenta en las normas, procesos, roles, responsabilidades y mecanismos regulados e implementados a nivel nacional en materia de Seguridad de la Información.

La Seguridad de la Información se enfoca en la información, de manera independiente de su formato y soporte. La seguridad digital se ocupa de las medidas de la seguridad de la información procesada, transmitida, almacenada o contenida en el entorno digital, procurando generar confianza, gestionando los riesgos que afecten la seguridad de las personas y la prosperidad económica y social en dicho entorno.

Artículo 34. Financiamiento

La implementación de lo establecido en el presente Decreto Legislativo se financia con cargo al presupuesto institucional de las entidades involucradas, sin demandar recursos adicionales al Tesoro Público.

Artículo 35. Refrendo

El presente Decreto Legislativo es refrendado por el Presidente del Consejo de Ministros y el Ministro de Justicia y Derechos Humanos.

DISPOSICIONES COMPLEMENTARIAS FINALES

Primera. Reglamentación

La Presidencia del Consejo de Ministros, mediante Decreto Supremo, aprueba el Reglamento del presente Decreto Legislativo en un plazo máximo de ciento ochenta (180) días, contados a partir del día siguiente de su publicación en el Diario Oficial El Peruano.

Segunda. Normas sobre Identidad Digital Nacional

El Registro Nacional de Identificación y Estado Civil (RENIEC) en el ámbito de sus funciones y competencias emitirá las normas que resulten pertinentes para el otorgamiento, registro y acreditación de la identidad digital nacional. La Identidad Digital Nacional proporciona el mismo valor legal que el Documento Nacional de Identidad.

Tercera. Fortalecimiento de capacidades

La Autoridad Nacional del Servicio Civil (SERVIR) en el ámbito de sus funciones y competencias, en coordinación con la Secretaría de Gobierno Digital, promueve el fortalecimiento de capacidades en materia de gobierno digital y tecnologías digitales a los funcionarios y servidores de las entidades de la Administración Pública.

Cuarta. Registro de Centros de Acceso Público

Las entidades de la Administración Pública que implementan progresivamente, en función a sus recursos y capacidades, espacios o centros de acceso público, previstos en la Ley de Promoción de Banda Ancha y

Construcción de la Red Dorsal Nacional de Fibra Óptica, con miras a fortalecer capacidades y facilitar el proceso de inclusión digital de los ciudadanos y personas en general el acceso a los servicios digitales deben comunicarlo a la Secretaría de Gobierno Digital para el registro respectivo.

Entiéndase que toda referencia a los Centros de Acceso Ciudadano previstos en el Reglamento de la Ley de Firmas y Certificados Digitales se entenderá hecha al Centro de Acceso Público previsto en la presente norma.

Quinta. Vigencia

El presente Decreto Legislativo entra en vigencia a partir del día siguiente de su publicación, con excepción de lo previsto en los artículos 11, 12, 14, 15, 19, 20, 21, 22, 25, 27, 31 y numerales 18.1, 18.5, 18.6 y 18.8 del artículo 18, que entrarán en vigor con la norma reglamentaria correspondiente.

DISPOSICIONES COMPLEMENTARIAS TRANSITORIAS

Primera. Credencial de Identidad Digital

Las entidades de la Administración Pública pueden hacer uso de los mecanismos existentes para la autenticación de las personas en entornos digitales dentro de un contexto determinado, conforme a los lineamientos, progresividad y plazos a establecerse en el reglamento del presente Decreto Legislativo.

Segunda. Servicios Digitales

Las entidades de la Administración Pública que a la fecha de entrada en vigencia del presente Decreto Legislativo hayan implementado y brinden servicios digitales adoptan y adecuan las disposiciones de los mismos de manera progresiva conforme a sus recursos, capacidades, lineamientos y plazos a establecerse en el reglamento de la presente Ley, sin perjuicio de lo establecido en el numeral 5.1 del artículo 5 del presente Decreto Legislativo.

Resolución Legislativa 30913. Resolución Legislativa que aprueba el Convenio sobre la Ciberdelincuencia (Convenio de Budapest)

Artículo Único. Aprobación del Convenio

Apruébase el Convenio sobre la Ciberdelincuencia, adoptado en Budapest el 23 de noviembre de 2001, con las siguientes declaraciones y reservas:

DECLARACIONES

a. De conformidad con lo dispuesto en el artículo 2 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que su legislación exige que el delito de acceso ilícito se cometa infringiendo medidas de seguridad.

b. De conformidad con lo dispuesto en el artículo 3 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que su legislación exige que el delito de interceptación ilícita se cometa con intención delictiva y que dicho delito puede cometerse en relación con un sistema informático conectado a otro sistema informático.

c. De conformidad con lo dispuesto en el artículo 7 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que podrá exigir que exista una intención fraudulenta o delictiva similar, conforme a lo establecido en su derecho interno, para que las conductas descritas en dicho artículo generen responsabilidad penal.

d. De conformidad con lo establecido en el artículo 27, numeral 9, literal e) del Convenio sobre la Ciberdelincuencia, la República del Perú declara que, en aras de la eficacia, las solicitudes efectuadas en virtud de lo dispuesto en el literal e) del numeral 9 del citado artículo del Convenio deberán dirigirse a su autoridad central.

RESERVAS

a. De conformidad con lo dispuesto en el párrafo 3 del artículo 6 del Convenio sobre la Ciberdelincuencia, la

República del Perú se reserva el derecho de no aplicar el artículo 6, párrafo 1, literal b del Convenio.

b. De conformidad con el numeral 4 del artículo 9 del Convenio sobre la Ciberdelincuencia, la República del Perú considera que el bien jurídico tutelado en el derecho interno con respecto a la pornografía infantil es la libertad y/o indemnidad sexual de un menor, por lo que formula una reserva a los literales b) y c) del párrafo 2 del citado artículo, debido a que las conductas contempladas en dichas disposiciones no involucran la participación de un menor de edad.

c. Conforme al numeral 4 del artículo 29 del Convenio sobre la Ciberdelincuencia, la República del Perú se reserva el derecho a denegar la solicitud de conservación en virtud de dicho artículo en el caso que tenga motivos para creer que, en el momento de la revelación de los datos, no se cumplirá con la condición de la doble tipificación penal.

Ley 3099, Ley de Ciberdefensa

TÍTULO I

DISPOSICIONES GENERALES

Artículo 1. Objeto

La presente ley tiene por objeto establecer el marco normativo en materia de ciberdefensa del Estado peruano, regulando las operaciones militares en y mediante el ciberespacio a cargo de los órganos ejecutores del Ministerio de Defensa dentro de su ámbito de competencia, conforme a ley.

Artículo 2. Finalidad

Defender y proteger la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves para mantener las capacidades nacionales frente a amenazas o ataques en y mediante el ciberespacio, cuando estos afecten la seguridad nacional.

Artículo 3. Ámbito de aplicación

El ámbito de aplicación de la norma se circunscribe a la ejecución de operaciones de ciberdefensa en y mediante el ciberespacio frente a las amenazas o los ataques que afecten la seguridad nacional.

Artículo 4. Definición

Entiéndase por ciberdefensa a la capacidad militar que permite actuar frente a amenazas o ataques realizados en y mediante el ciberespacio cuando estos afecten la seguridad nacional.

Artículo 5. Órganos ejecutores

Las Fuerzas Armadas, que están constituidas por el Ejército, la Marina de Guerra y la Fuerza Aérea, y el Comando Conjunto de las Fuerzas Armadas son instituciones con calidad de órganos ejecutores del Ministerio de Defensa.

TÍTULO II

DE LA CIBERDEFENSA

CAPÍTULO I

LAS CAPACIDADES DE CIBERDEFENSA Y LAS OPERACIONES EN Y MEDIANTE EL CIBERESPACIO

Artículo 6. De las capacidades de ciberdefensa

> Es el uso de conocimiento, habilidades y medios para realizar operaciones en y mediante el ciberespacio a fin de asegurar su empleo por las fuerzas propias.

Artículo 7. De las operaciones militares en el ciberespacio

> Es el eficiente y eficaz empleo de las capacidades de ciberdefensa por parte de los órganos ejecutores del Ministerio de Defensa, de acuerdo a sus funciones y en el ámbito de sus respectivas competencias, contra las amenazas o los ataques en y mediante el ciberespacio, cuando estos afecten la seguridad nacional.

Artículo 8. De la planificación y ejecución de las operaciones en el ciberespacio

> La planificación y ejecución de las operaciones de ciberdefensa a cargo del Comando Conjunto de las Fuerzas Armadas responde al mandato conferido en la Constitución Política del Perú, así como al cumplimiento de las responsabilidades asignadas en las leyes que regulan su naturaleza jurídica, competencias, funciones y estructura orgánica, las disposiciones contenidas en la presente ley, y los tratados y acuerdos internacionales de los que el Perú es parte y resulten aplicables.

CAPÍTULO II

DEL USO DE LA FUERZA EN Y MEDIANTE EL CIBERESPACIO

Artículo 9. Del uso de la fuerza por las Fuerzas Armadas

El uso de la fuerza por la Fuerzas Armadas en y mediante el ciberespacio se sujeta a las disposiciones contenidas en el artículo 51 de la Carta de las Naciones Unidas y el presente dispositivo legal, y está regido por las normas del Derecho Internacional de los Derechos Humanos y del Derecho Internacional Humanitario que sean aplicables.

Artículo 10. De la legítima defensa

Toda amenaza o ataque en y mediante el ciberespacio que ponga en riesgo la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves para mantener las capacidades nacionales, da lugar al ejercicio del derecho de legítima defensa.

Artículo 11. Requisitos para el ejercicio del uso de la fuerza

El ejercicio del derecho de legítima defensa en el contexto de las operaciones de ciberdefensa está sujeto a los principios de legalidad, necesidad y oportunidad.

En el caso de conducir una operación de respuesta en y mediante el ciberespacio que contenga un ataque deliberado, debe realizarse de acuerdo a ley.

CAPÍTULO III

DE LA SEGURIDAD DE LOS ACTIVOS CRÍTICOS NACIONALES Y RECURSOS CLAVES

Artículo 12. Del control y de la protección de los activos críticos nacionales y recursos claves

El Comando Conjunto de las Fuerzas Armadas está a cargo de la ciberdefensa de los activos críticos nacionales y recursos claves, cuando la capacidad de protección de sus operadores y/o del sector responsable de cada uno de ellos y/o de la Dirección Nacional de Inteligencia sea sobrepasada, a fin de mantener las capacidades nacionales, en el ámbito de la seguridad nacional.

Artículo 13. De los protocolos de escalamiento, coordinación, intercambio y activación

La Presidencia del Consejo de Ministros, en su calidad de miembro del Consejo de Seguridad y Defensa Nacional, establece los protocolos de escalamiento, coordinación, intercambio y activación para lo indicado en la presente ley.

Esta función se ejerce a través de la Secretaría de Gobierno Digital en su calidad de ente rector del Sistema Nacional de Informática y de la seguridad digital en el país, quien emite los lineamientos y las directivas correspondientes.

Artículo 14. Modificación del artículo 32 del Decreto Legislativo 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital

Modifícase el artículo 32 del Decreto Legislativo 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, el cual queda redactado de la siguiente manera:

"Artículo 32. Gestión del Marco de Seguridad Digital del Estado Peruano

El Marco de Seguridad Digital del Estado Peruano tiene los siguientes ámbitos:

a. Defensa: El Ministerio de Defensa (MINDEF), en el marco de sus funciones y competencias, dirige, norma, supervisa y evalúa las normas en materia de ciberdefensa.

[…]."

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA. Reglamentación en materia de ciberdefensa

La Presidencia del Consejo de Ministros, en coordinación con el Ministerio de Defensa, aprueba el reglamento de la presente ley, en un plazo máximo de noventa (90) días, contados a partir del día siguiente de su publicación en el diario oficial El Peruano.

SEGUNDA. Modificaciones a normas de las Fuerzas Armadas en materia de ciberdefensa

El Ministerio de Defensa, en un plazo de noventa (90) días, contados a partir de la fecha de entrada en vigencia de la presente ley, presenta las modificaciones, derogaciones e incorporaciones a las normas correspondientes a las Fuerzas Armadas en materia de la presente ley.

TERCERA. Recursos críticos de Internet

Se reconoce a las entidades que gestionen recursos críticos de Internet (nombres de dominio, números IP y protocolos) en su naturaleza de entidades vinculadas a la ciberdefensa, debiendo mantener mecanismos de comunicación de incidentes que pudieran afectar la capacidad de ciberdefensa nacional.

CUARTA. Desarrollo de currículos de educación superior en materia de ciberdefensa

La Presidencia del Consejo de Ministros, en su calidad de ente rector en materia de seguridad digital, coordina con el Ministerio de Defensa y el Ministerio de Educación la pertinencia del desarrollo de contenidos especializados en materia de seguridad digital, que incluye la ciberdefensa, en las instituciones de educación superior universitaria y tecnológica, a nivel de pregrado y postgrado. Para ello, establece instrumentos de cooperación interinstitucional con entidades del sector privado, la academia, la sociedad civil y la comunidad técnica.

QUINTA. Aplicación de recursos especiales

Los procesos para las capacidades de ciberdefensa deben considerarse dentro del alcance de la aplicación de los artículos 30 y 31 del Decreto Legislativo 1141.

DISPOSICIÓN COMPLEMENTARIA DEROGATORIA

ÚNICA. Derogatoria

> Deróganse o déjense en suspenso, según el caso, las disposiciones legales y reglamentarias que se opongan a lo establecido por la presente ley o limiten su aplicación, con la entrada en vigencia de la presente ley.

Decreto de Urgencia 007-2020. Decreto de Urgencia que aprueba el marco de Confianza Digital y dispone medidas para su fortalecimiento

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1. Objeto

> El presente Decreto de Urgencia tiene por objeto establecer las medidas que resultan necesarias para garantizar la confianza de las personas en su interacción con los servicios digitales prestados por entidades públicas y organizaciones del sector privado en el territorio nacional.

Artículo 2. Alcance

> Las normas y procedimientos que rigen la materia de Confianza Digital son aplicables a las entidades establecidas en el artículo I del Título Preliminar del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado mediante Decreto Supremo N° 004-2019-JUS, y, a las organizaciones de la sociedad civil, ciudadanos, empresas y academia.

Artículo 3. Definiciones

Para la aplicación del presente Decreto de Urgencia se establece las siguientes definiciones:

a) Confianza Digital. Es el estado que emerge como resultado de cuán veraces, predecibles, éticas, proactivas, transparentes, seguras, inclusivas y confiables son las interacciones digitales que se generan entre personas, empresas, entidades públicas o cosas en el entorno digital, con el propósito de impulsar el desarrollo de la economía digital y la transformación digital. Es un componente de la transformación digital y tiene como ámbitos la protección de datos personales, la ética, la transparencia, la seguridad digital y la protección del consumidor en el entorno digital.

b) Economía digital. Es la innovación y la transformación de la economía basada en el uso estratégico y disruptivo de las tecnologías digitales. Desarrolla la capacidad de incrementar la eficiencia, productividad, transparencia, seguridad y eficacia de los procesos y actividades económicas y sociales, sustentada en el uso intensivo de tecnologías digitales, redes de datos o comunicación y plataformas digitales. Conlleva a la generación de beneficios económicos y sociales, prosperidad y bienestar para la sociedad.

c) Entorno Digital. Es el dominio o ámbito habilitado por las tecnologías y dispositivos digitales, generalmente interconectados a través de redes e infraestructuras de datos o comunicación, incluyendo el Internet, que soportan los procesos, servicios, plataformas que sirven como base para la interacción entre personas, empresas, entidades públicas o dispositivos.

d) Actividad crítica. Es la actividad económica y/o social cuya interrupción tiene graves consecuencias en la salud y seguridad de los ciudadanos, en el funcionamiento efectivo de los servicios esenciales que mantienen la economía, sociedad y el gobierno, o afectan la prosperidad económica y social en general.

e) Incidente de seguridad digital. Evento o serie de eventos que pueden comprometer la confianza, la prosperidad económica, la protección de las personas y sus datos personales, la información, entre otros activos de la organización, a través de tecnologías digitales.

f) Gestión de incidentes de seguridad digital. Proceso formal que tiene por finalidad planificar, preparar, identificar, analizar, contener, investigar incidentes de seguridad digital, así como la recuperación y la determinación de acciones correctivas para prevenir incidentes similares.

g) Riesgo de seguridad digital. Efecto de la incertidumbre relacionada con el uso, desarrollo y gestión de las tecnologías digitales y datos, en el curso de cualquier actividad. Resulta de la combinación de amenazas y vulnerabilidades en el entorno digital y es de naturaleza dinámica. Puede socavar el logro de los objetivos económicos y sociales al alterar la confidencialidad, integridad y disponibilidad de las actividades o el entorno, así como poner en riesgo la protección de la vida privada de las personas. Incluye aspectos relacionados con los entornos físicos y digitales, las actividades críticas, las personas y organizaciones involucradas en la actividad y los procesos organizacionales que la respaldan.

h) Ciberseguridad. Capacidad tecnológica de preservar el adecuado funcionamiento de las redes, activos y sistemas informáticos y protegerlos ante amenazas y vulnerabilidades en el entorno digital. Comprende la perspectiva técnica de la Seguridad Digital y es un ámbito del Marco de Seguridad Digital del país.

i) Servicio digital. Es aquel servicio provisto de forma total o parcial a través de Internet u otras redes equivalentes, que se caracteriza por ser parcial o totalmente automatizado y utilizar de manera intensiva las tecnologías digitales y datos, permitiendo,

al menos una de las siguientes prestaciones: i) Adquirir un bien, servicio, información o contenido, ii) Buscar, compartir, usar y acceder a datos, contenido o información sobre productos, servicios o personas, iii) Pagar un servicio o bien (tangible o intangible) y, iv) El relacionamiento entre personas.

j) Proveedor de servicios digitales. Comprende a cualquier entidad pública u organización del sector privado, independientemente de su localización geográfica, que sea responsable por el diseño, prestación y/o acceso a servicios digitales en el territorio nacional.

CAPÍTULO II

MARCO DE CONFIANZA DIGITAL

Artículo 4. Marco de Confianza Digital

4.1 El Marco de Confianza Digital se constituye en el conjunto de principios, modelos, políticas, normas, procesos, roles, personas, empresas, entidades públicas, tecnologías y estándares mínimos que permiten asegurar y mantener la confianza en el entorno digital.

4.2 El Marco de Confianza Digital tiene los siguientes ámbitos:

a) Protección de datos personales y transparencia. El Ministerio de Justicia y Derechos Humanos (MINJUSDH), quien ejerce las autoridades nacionales de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, en el marco de sus funciones y competencias, norma, dirige, supervisa y evalúa la materia de transparencia y protección de datos personales.

b) Protección del consumidor. El Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI), en el marco de sus funciones y competencias, norma, dirige, supervisa y evalúa la materia de protección al consumidor.

c) Seguridad Digital. La Presidencia del Consejo de Ministros (PCM), a través de la Secretaría de Gobierno Digital, en su calidad de ente rector de seguridad digital en el país, norma, dirige, supervisa y evalúa la materia de seguridad digital.

Artículo 5. Ente rector del Marco de Confianza Digital

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el ente rector en materia de Confianza Digital y responsable de la articulación de cada uno de sus ámbitos.

Artículo 6. Atribuciones del Ente rector

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, en su calidad de ente rector de la Confianza Digital, tiene las siguientes funciones:

a) Formular, articular y dirigir la estrategia de Confianza Digital a nivel nacional, y supervisar su cumplimiento.

b) Emitir lineamientos, estándares, especificaciones, guías, directivas, normas técnicas y estándares en materia de Confianza digital, sin que ello afecte el equilibrio económico financiero de los proyectos digitales.

c) Evaluar las necesidades de las entidades públicas, organizaciones privadas y personas en materia de Confianza Digital.

d) Articular acciones y medidas para la implementación de la estrategia de Confianza Digital a nivel nacional con actores del sector público, sector privado, sociedad civil, academia y otros interesados, así como promover reconocimientos.

e) Mantener informado al Presidente del Consejo de Ministros sobre los resultados y avances de la Confianza Digital en el país y los incidentes de seguridad digital notificados en el Centro Nacional de Seguridad Digital cuando corresponda.

Dichas funciones se ejercen sin afectar las autonomías y atribuciones de cada sector en el marco de sus competencias.

Artículo 7. Centro Nacional de Seguridad Digital

7.1 Créase el Centro Nacional de Seguridad Digital como una plataforma digital que gestiona, dirige, articula y supervisa la operación, educación, promoción, colaboración y cooperación de la Seguridad Digital a nivel nacional como componente integrante de la seguridad nacional, a fin de fortalecer la confianza digital. Asimismo, es responsable de identificar, proteger, detectar, responder, recuperar y recopilar información sobre incidentes de seguridad digital en el ámbito nacional para gestionarlos.

7.2 El Centro Nacional de Seguridad Digital se encuentra a cargo de la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, y es el único punto de contacto nacional en las comunicaciones y coordinaciones con otros organismos, centros o equipos nacionales e internacionales de similar naturaleza.

7.3 El Centro Nacional de Seguridad Digital constituye el mecanismo de intercambio de información y articulación de acciones con los responsables de los ámbitos del Marco de Seguridad Digital del Estado Peruano, de conformidad con el artículo 32 del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.

7.4 El Centro Nacional de Seguridad Digital incorpora al Equipo de Respuesta a Incidentes de Seguridad Digital Nacional responsable de: i) Gestionar la respuesta y/o recuperación ante incidentes de seguridad digital en el ámbito nacional y, ii) Coordinar y articular acciones con otros equipos de similar naturaleza nacionales e internacionales para atender los incidentes de seguridad digital

7.5 La Secretaría de Gobierno Digital establece los protocolos de escalamiento, coordinación, intercambio y activación ante incidentes de seguridad digital en el país y emite los lineamientos y las directivas correspondientes.

CAPÍTULO III

MEDIDAS PARA FORTALECER LA CONFIANZA DIGITAL

Artículo 8. Registro Nacional de Incidentes de Seguridad Digital

8.1 Créase el Registro Nacional de Incidentes de Seguridad Digital que tiene por objetivo recibir, consolidar y mantener datos e información sobre los incidentes de seguridad digital reportados por los proveedores de servicios digitales en el ámbito nacional que puedan servir de evidencia o insumo para su análisis, investigación y solución.

8.2 El Registro Nacional de Incidentes de Seguridad Digital y la información contenida en el mismo tiene carácter confidencial, se soporta en una plataforma digital administrada por la Secretaría de Gobierno Digital, quien es responsable de su disponibilidad, confidencialidad e integridad.

8.3 El Centro Nacional de Seguridad Digital brinda información sobre los registros de incidentes de seguridad digital, a los responsables de los ámbitos del Marco de Seguridad Digital, de conformidad con el artículo 32 del Decreto Legislativo N° 1412, y del Marco de Confianza Digital debiendo observar para tal efecto la normatividad vigente en materia de protección de datos personales.

Artículo 9. Obligaciones del Proveedor de servicios digitales

9.1 Las entidades de la administración pública, los proveedores de servicios digitales del sector financiero, servicios básicos (energía eléctrica, agua y gas), salud y transporte de personas, proveedores de servicios de internet, proveedores de actividades críticas y de servicios educativos, deben:

a) Notificar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital.

b) Implementar medidas de seguridad física, técnica, organizativa y legal que permitan garantizar la

confidencialidad del mensaje, contenido e información que se transmiten a través de sus servicios de comunicaciones.

c) Gestionar los riesgos de seguridad digital en su organización con fines de establecer controles que permitan proteger la confidencialidad, integridad y disponibilidad de la información.

d) Establecer mecanismos para verificar la identidad de las personas que acceden a un servicio digital, conforme al nivel de riesgo del mismo y de acuerdo a la normatividad vigente en materia de protección de datos personales.

e) Reportar y colaborar con la autoridad de la protección de datos personales cuando verifiquen un incidente de seguridad digital que involucre datos personales.

f) Mantener una infraestructura segura, escalable e interoperable.

9.2 Las organizaciones privadas toman como referencia las normas emitidas por la Secretaría de Gobierno Digital en cuanto les aplique y les genere valor e implementan de forma obligatoria aquellas que prevengan afectación a los derechos de las personas.

9.3 Las entidades de la administración pública deben implementar un Sistema de Gestión de Seguridad de la Información (SGSI), un Equipo de Respuestas ante Incidentes de Seguridad Digital cuando corresponda y cumplir con la regulación emitida por la Secretaría de Gobierno Digital.

9.4 Toda actividad crítica debe estar soportada en una infraestructura segura, disponible, escalable e interoperable.

Artículo 10. Articulación internacional

La Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros coordina con el Ministerio de Relaciones Exteriores las acciones vinculadas a la política

exterior que contribuyan a fortalecer la confianza en el entorno digital cuando corresponda y en el marco de sus competencias.

Artículo 11. Articulación en Materia de Comunicaciones

La Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros coordina con el Ministerio de Transportes y Comunicaciones las acciones vinculadas a la materia de comunicaciones en el marco de sus competencias.

CAPÍTULO IV

USO ÉTICO DE LAS TECNOLOGIA DIGITALES Y DE LOS DATOS

Artículo 12. Datos como activos estratégicos

12.1 Las entidades públicas y las organizaciones del sector privado administran los datos, en especial los datos personales, biométricos y espaciales, como activos estratégicos, garantizando que estos se generen, compartan, procesen, accesen, publiquen, almacenen, conserven y pongan a disposición durante el tiempo que sea necesario y cuando sea apropiado, considerando las necesidades de información, uso ético, transparencia, riesgos y el estricto cumplimiento de la normatividad en materia de protección de datos personales, gobierno digital y seguridad digital.

12.2 Las entidades públicas y las organizaciones del sector privado promueven y aseguran el uso ético de tecnologías digitales, el uso intensivo de datos, como internet de las cosas, inteligencia artificial, ciencia de datos, analítica y procesamiento de grandes volúmenes de datos.

12.3 El tratamiento de datos personales debe cumplir la legislación de la materia emitida por la Autoridad Nacional de Protección de Datos Personales.

Artículo 13. Centro Nacional de Datos

13.1 Créase el Centro Nacional de Datos como una plataforma digital que gestiona, dirige, articula y supervisa la operación, educación, promoción, colaboración y cooperación de datos a nivel nacional, a fin de fortalecer la confianza y bienestar de las personas en el entorno digital en el marco de la presente norma.

13.2 El Centro Nacional de Datos se encuentra a cargo de la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital y es el único punto de contacto nacional en las comunicaciones y coordinaciones con otros organismos, centros o equipos nacionales e internacionales de similar naturaleza.

13.3 El Centro Nacional de Datos intercambia información y articula acciones con las entidades públicas, academia, sociedad civil y sector privado y con las entidades responsables de los ámbitos del Marco de Confianza Digital para la gobernanza de datos.

13.4 La Secretaría de Gobierno Digital, en su calidad de ente rector en gobernanza de datos, establece los protocolos y mecanismos en materia de gobierno de datos y emite los lineamientos y las directivas correspondientes.

Artículo 14. Financiamiento

La implementación de lo establecido en el presente Decreto de Urgencia se financia con cargo al presupuesto institucional de las entidades involucradas, sin demandar recursos adicionales al Tesoro Público.

Artículo 15. Refrendo

El presente Decreto de Urgencia es refrendado por el Presidente del Consejo de Ministros y la Ministra de Justicia y Derechos Humanos.

DISPOSICIONES COMPLEMENTARIAS FINALES

Primera. Reglamentación

El Poder Ejecutivo, dentro de los noventa (90) días hábiles siguientes a la entrada en vigencia de la presente norma, aprueba su reglamento mediante Decreto Supremo refrendado por el Presidente del Consejo de Ministros.

Segunda. Registro Nacional de Incidentes de Seguridad Digital

En un plazo no mayor a noventa (90) días hábiles, posterior a la publicación del presente Decreto de Urgencia, la Presidencia del Consejo de Ministros implementa el Registro Nacional de Incidentes de Seguridad Digital y dicta normas, lineamientos y directivas para su correcto funcionamiento.

Tercera. Gestión e Impulso de la Red Nacional de Estado Peruano (REDNACE) y la Red Nacional de Investigación y Educación (RNIE)

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, se encarga de la gestión e impulso de la Red Nacional de Estado Peruano (REDNACE) y la Red Nacional de Investigación y Educación (RNIE) a las que se refiere la Ley N° 29904 a fin de coadyuvar al logro de las políticas nacionales, el fortalecimiento de una sociedad digital y la transformación digital del Estado. La contratación de los servicios para la conectividad de la REDNACE es realizada por cada entidad de la Administración Pública, de conformidad con lo dispuesto en el artículo 19 de dicha Ley.

Cuarta. Aplicación de la Norma

La presente norma se aplica a los proyectos de asociación público privada, contratos de concesión, proyectos incorporados al proceso de promoción de la inversión privada u otros proyectos y plataformas sobre transformación digital que se diseñen, inicien o gestionen a partir de la entrada en vigencia de la misma.

DS 029-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo

(…)

TÍTULO VII

SEGURIDAD DIGITAL

CAPÍTULO I

MARCO DE SEGURIDAD DIGITAL DEL ESTADO PERUANO

Artículo 94. Marco de Seguridad Digital del Estado Peruano

94.1 El Marco de Seguridad Digital del Estado Peruano es dirigido, supervisado y evaluado por la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, en su calidad de ente rector de la seguridad digital, que emite lineamientos, especificaciones, guías, directivas, normas técnicas y estándares para su aplicación por parte de las entidades de la Administración Pública a fin de fortalecer la confianza de los ciudadanos, entidades públicas y personas en general en el entorno digital.

94.2 El Marco de Seguridad Digital del Estado Peruano integra aquellas normas que conforman los ámbitos de defensa, inteligencia, justicia e institucional, establecidos en el artículo 32 de la Ley y se articula y sustenta en las normas, procesos, roles, responsabilidades y mecanismos regulados e implementados a nivel nacional en materia de Seguridad de la Información. La seguridad digital es un ámbito del Marco de Confianza Digital establecido en el Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.

94.3 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es la encargada de: (1) definir, articular y dirigir la política, estrategia y planes para el desarrollo de la Seguridad Digital del Estado Peruano, (2) emitir lineamientos, especificaciones, guías, directivas, normas técnicas y estándares en Seguridad Digital, (3) supervisar su cumplimiento, (4) evaluar las necesidades de las entidades, ciudadanos y personas en general en dicho ámbito, (5) asesorar el Consejo de Seguridad y Defensa Nacional sobre los aspectos relacionados a seguridad digital, (6) impulsar campañas de sensibilización sobre los riesgos de seguridad digital de la ciudadanía, (7) promover contenidos digitales para la formación de talento digital en seguridad y, (8) comunicar al Presidente del Consejo de Ministros los resultados y avances del mismo, a fin de garantizar de manera efectiva la seguridad digital en el país.

Artículo 95. Principios del Marco de Seguridad Digital del Estado Peruano

La aplicación del Marco de Seguridad Digital del Estado Peruano se desarrolla de acuerdo con los principios rectores establecidos en el artículo 5 de la Ley, y con los siguientes principios específicos de la seguridad digital:

a) Seguridad desde el diseño. Los servicios digitales se diseñan y crean atendiendo las necesidades de disponibilidad, integridad y confidencialidad de los datos e información que capturan, procesan y distribuyen.

b) Gestión de riesgos. La gestión de riesgos de seguridad en el entorno digital está integrada en la toma de decisiones, diseño de controles de seguridad en los servicios digitales y procesos de la entidad. Es responsabilidad de la alta dirección dirigirla, mantenerla e incorporarla en la gestión integral de riesgos de la entidad.

c) Colaboración y cooperación. Se promueve el intercambio de información, mejores prácticas y

experiencias a fin de identificar y prevenir riesgos de seguridad digital; así como detectar, responder y recuperarse ante incidentes en el entorno digital que afecten la continuidad de las entidades, bienestar de las personas y el desarrollo sostenible del país.

d) Participación responsable. El Estado y la sociedad en su conjunto tienen responsabilidad en la protección de sus datos personales y gestión de riesgos en el entorno digital, en función de sus roles, contexto y su capacidad de actuar, teniendo en cuenta el impacto potencial de sus decisiones con respecto a otros.

e) Protección de datos e información. Se promueve la implementación de medidas y controles de seguridad organizativos, técnicos y legales para preservar la disponibilidad, integridad y confidencialidad de los datos e información que capture, procese, almacene y distribuya una entidad, así como en cualquier otra forma de actividad que facilite el acceso o la interconexión de los datos.

f) Enfoque nacional. La Seguridad Digital es un componente de la seguridad nacional, respalda el funcionamiento del Estado, la sociedad, la competitividad, la economía y la innovación.

g) Enfoque integral. La Seguridad Digital es entendida como un proceso integral y holístico constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con una entidad.

Artículo 96. Modelo de Seguridad Digital

96.1 El Modelo de Seguridad Digital es la representación holística y sistémica de los componentes que comprende el Marco de Seguridad Digital del Estado Peruano, atendiendo los principios establecidos en el artículo 95 del presente Reglamento, aquellos establecidos en la Ley, el Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone

medidas para su fortalecimiento, y las normas en materia de Seguridad de la Información en el Estado Peruano.

96.2 El Modelo de Seguridad Digital comprende los siguientes componentes:

a) Responsables de los ámbitos del Marco de Seguridad Digital.

b) Centro Nacional de Seguridad Digital.

c) Redes de confianza en Seguridad Digital.

d) Oficial de Seguridad Digital.

e) Sistemas de Gestión de Seguridad de la Información.

f) Ciudadano o persona en general.

g) Autoridad Nacional de Protección de Datos Personales.

Artículo 97. Articulación normativa en materia de Seguridad Digital

Las políticas, lineamientos, directrices y planes en los ámbitos de defensa, inteligencia, justicia e institucional previstos en el artículo 32 de la Ley, se articulan con las políticas, estrategias y planes en materia de Seguridad Digital del Estado Peruano que establezca la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital.

CAPÍTULO II

GESTIÓN DEL MARCO DE SEGURIDAD DIGITAL DEL ESTADO PERUANO

Artículo 98. Ámbito de Defensa

98.1 La ciberdefensa es gestionada por el Ministerio de Defensa, quien articula con sus órganos ejecutores el planeamiento y conducción de operaciones militares en y mediante el ciberespacio conforme los objetivos y lineamientos de la Política de Seguridad y Defensa

Nacional aprobados por el Consejo de Seguridad y Defensa Nacional (COSEDENA) y de manera articulada con los objetivos de seguridad digital.

98.2 El Comando Conjunto de las Fuerzas Armadas está a cargo de la ciberdefensa de los activos críticos nacionales y recursos claves, cuando la capacidad de protección de sus operadores y/o sector responsable de cada uno de ellos o de la Dirección Nacional de Inteligencia o quien haga sus veces, sean sobrepasadas, y se vea afectada la seguridad nacional.

98.3 La Presidencia del Consejo de Ministros, en su calidad de miembro del Consejo de Seguridad y Defensa Nacional, establece los protocolos de escalamiento, coordinación, intercambio y activación para lo indicado en la Ley Nº 30999, Ley de Ciberdefensa. Esta función se ejerce a través de la Secretaría de Gobierno Digital en su calidad de ente rector del Sistema Nacional de Transformación Digital y de seguridad y confianza digital en el país, quien emite los lineamientos y las directivas correspondientes.

Artículo 99. Ámbito de Inteligencia

La inteligencia y contrainteligencia en este ámbito es gestionada, en el marco de sus competencias, por la Dirección Nacional de Inteligencia (DINI), quien articula con la Secretaría de Gobierno Digital Presidencia del Consejo de Ministros y los órganos competentes, el planeamiento y conducción de operaciones de inteligencia para asegurar los activos críticos nacionales.

Artículo 100. Ámbito de Justicia

100.1 Las acciones para garantizar la lucha eficaz contra la ciberdelincuencia es dirigida por el Ministerio del Interior (MININTER) y la Policía Nacional del Perú (PNP), quienes articulan con el Ministerio de Justicia y Derechos Humanos (MINJUSDH), el Instituto Nacional

Penitenciario (INPE), el Ministerio Público - Fiscalía de la Nación, el Tribunal Constitucional, Academia de la Magistratura, la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros y el Poder Judicial (PJ), conforme a lo dispuesto en la Ley Nº 30096, Ley de Delitos Informáticos, y los convenios aprobados y ratificados por el Estado Peruano en esta materia.

100.2 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, en coordinación con la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) de la Policía Nacional del Perú y el Ministerio Público - Fiscalía de la Nación proponen los protocolos de colaboración y comunicación para el reporte de casos de violencia sexual contra niños, niñas y adolescentes en el entorno digital, la cual se hace efectiva mediante Resolución de la Secretaría de Gobierno Digital.

Artículo 101. Ámbito Institucional

El ámbito institucional es dirigido, evaluado y supervisado por la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, quien articula con las entidades de la Administración Pública la implementación de las normas, directivas y estándares de Seguridad Digital, Ciberseguridad y Seguridad de la Información, y supervisa su cumplimiento.

Artículo 102. Articulación de ámbitos

La Secretaría de Gobierno Digital dirige y articula acciones para la gestión de incidentes y riesgos de seguridad digital que afecten a la sociedad con los responsables de los ámbitos de Defensa, Inteligencia y Justicia, conforme lo establece el Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento y su Reglamento.

Artículo 103. Adopción de estándares y buenas prácticas

Las entidades de la Administración Pública pueden adoptar normas técnicas peruanas o normas y/o estándares técnicos internacionales ampliamente reconocidos en materia de gestión de riesgos, gestión de incidentes, seguridad digital, ciberseguridad y seguridad de la información en ausencia de normas o especificaciones técnicas nacionales vigentes.

CAPÍTULO III

EQUIPO DE RESPUESTAS ANTE INCIDENTES DE SEGURIDAD DIGITAL

Artículo 104. Equipo de Respuestas ante Incidentes de Seguridad Digital

104.1 Un Equipo de Respuestas ante Incidentes de Seguridad Digital es aquel equipo responsable de la gestión de incidentes de seguridad digital que afectan los activos de una entidad pública o una red de confianza. Su implementación y conformación se realiza en base a las disposiciones que determine la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros.

104.2 Las entidades de la Administración pública conforman un Equipo de Respuestas ante Incidentes de Seguridad Digital de carácter institucional. Dichos Equipos forman parte de los órganos o unidades orgánicas de Tecnologías de la Información de la entidad o de la unidad de organización especializada en seguridad de la información o similar prevista en su estructura orgánica o funcional. Su conformación es comunicada a la Secretaría de Gobierno Digital mediante los mecanismos dispuestos para tal fin.

104.3 La Secretaría de Gobierno Digital, en su calidad de ente rector de la seguridad digital en el país, emite opinión técnica especializada a pedido de una entidad a fin de revisar o validar aspectos técnicos sobre la conformación de un Equipo de Respuesta ante incidentes de Seguridad

Digital, conforme a lo establecido en el presente Reglamento y normas complementarias.

104.4 La red de confianza es el conjunto de entidades públicas e interesados que articulan acciones para el intercambio de información sobre incidentes de seguridad digital, vulnerabilidades, amenazas, medidas de mitigación, herramientas, mejores prácticas o similares en materia de seguridad digital. Se conforman en función de un sector, territorio o para atender un objetivo específico.

104.5 Las entidades públicas pueden conformar una red de confianza en base a las disposiciones establecidas por la Secretaría de Gobierno Digital. Asimismo, la Secretaría de Gobierno Digital en función de los objetivos nacionales, políticas de estado o aspectos estratégicos promueve la conformación de redes de confianza.

Artículo 105. Obligaciones de las entidades en Seguridad Digital

Las entidades públicas tienen, como mínimo, las siguientes obligaciones:

a) Implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI).

b) Comunicar al Centro Nacional de Seguridad Digital los incidentes de seguridad digital atendiendo lo establecido en el artículo 107 del presente Reglamento.

c) Adoptar medidas para la gestión de riesgos e incidentes de seguridad digital que afecten a los activos de la entidad.

d) Difundir alertas tempranas, avisos e información sobre riesgos e incidentes de seguridad digital en su entidad y red de confianza.

e) Asegurar acciones de investigación y cooperación efectiva, eficiente y segura con el Centro Nacional de Seguridad Digital.

f) Proveer los recursos y medidas necesarias para asegurar la efectiva gestión de incidentes de seguridad digital.

g) Requerir a sus proveedores de desarrollo de software el cumplimiento de estándares, normas técnicas y mejores prácticas de seguridad ampliamente reconocidos.

Artículo 106. Criterios para determinar el impacto significativo de un incidente

Para determinar el impacto significativo de un incidente de seguridad digital se consideran, como mínimo, los siguientes criterios:

a) Perjuicio a la reputación.

b) Pérdida u obligación financiera.

c) Interrupción de las operaciones, procesos o actividades de la entidad.

d) Divulgación no autorizada de datos personales o información reservada, secreta o confidencial.

e) Daños personales (físico, psicológico o emocional).

Artículo 107. Comunicación de un incidente

La comunicación de un incidente de seguridad digital se realiza conforme a lo establecido en el Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, su Reglamento y normas complementarias.

Artículo 108. Incidentes de Seguridad Digital relativos a Datos Personales

Las entidades públicas comunican y colaboran con la Autoridad Nacional de Protección de Datos Personales ante la identificación de incidentes de seguridad digital que hayan afectado los datos personales, comunicándose en un plazo máximo de 48 horas, a partir de la toma de conocimiento de la brecha de seguridad.

CAPÍTULO IV

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Artículo 109. Sistema de Gestión de Seguridad de la Información

109.1 El Sistema de Gestión de Seguridad de la Información (SGSI) comprende el conjunto de políticas, lineamientos, procedimientos, recursos y actividades asociadas, que gestiona una entidad con el propósito de proteger sus activos de información, de manera independiente del soporte en que estos se encuentren. Asimismo, contempla la gestión de riesgos e incidentes de seguridad de la información y seguridad digital, la implementación efectiva de medidas de ciberseguridad, y acciones de colaboración y cooperación.

109.2 El diseño, implementación, operación y mejora del SGSI atiende a las necesidades de todas las partes interesadas de la entidad; asimismo, responde a los objetivos estratégicos, estructura, tamaño, procesos y servicios de la entidad. El SGSI comprende al Equipo de Respuesta ante Incidentes de Seguridad Digital.

109.3 Las entidades de la Administración Pública implementan un SGSI en su institución, teniendo como alcance mínimo sus procesos misionales y aquellos que son relevantes para su operación.

109.4 Se gestiona la implementación de controles y medidas de seguridad a nivel organizacional, técnico y legal, basadas en riesgos, a fin de garantizar la disponibilidad, integridad y confidencialidad de los datos personales que sean tratados, procesados, almacenados y compartidos a una entidad, así como en cualquier otra forma de actividad que facilite el acceso o intercambio de datos.

Artículo 110. Gestión de Riesgos de Seguridad Digital

Las entidades de la Administración Pública gestionan sus riesgos de seguridad digital, conforme a lo establecido en el

Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento y sus normas reglamentarias.

Artículo 111. Roles para la Seguridad de la Información

111.1 El titular de la entidad es responsable de la implementación del SGSI.

111.2 El Comité de Gobierno Digital es responsable de dirigir, mantener y supervisar el SGSI de la entidad.

111.3 El Oficial de Seguridad Digital es el rol responsable de coordinar la implementación y mantenimiento del SGSI en la entidad, atendiendo las normas en materia de seguridad digital, confianza digital y gobierno digital. La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, emite el perfil del Oficial de Seguridad Digital en la Administración Pública.

Artículo 112. Deberes y obligaciones del personal de la entidad

112.1 Las entidades públicas capacitan e informan a su personal sobre sus deberes y obligaciones en materia de seguridad de la información y seguridad digital, siendo estos últimos responsables de su aplicación en el ejercicio de sus funciones y actividades. Asimismo, las entidades fortalecen las competencias de su personal en el uso adecuado, eficiente y seguro de las tecnologías digitales, para lo cual pueden solicitar el soporte de la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital.

112.2 El personal de la entidad que accede a datos e información a través de aplicativos informáticos, sistemas de información o herramientas informáticas usa credenciales que permitan determinar: su identidad en un ámbito determinado, los tipos de derecho o privilegio de uso y accesos asignados, las actividades realizadas, a fin de establecer responsabilidades cuando corresponda.

Artículo 113. Auditorías de Seguridad de la Información

113.1 Las entidades públicas de manera permanente realizan como mínimo una auditoría externa anual a su SGSI. Los resultados de las auditorías constan como información documentada por la entidad.

113.2 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, solicita a las entidades públicas informes de las auditorías realizadas o sobre la aplicación efectiva de las normas en materia de seguridad de la información o seguridad digital, en el marco de sus funciones de supervisión o cuando lo considere necesario para prevenir o resolver incidentes de seguridad digital.

Artículo 114. Seguridad de los servicios digitales

Los servicios digitales se implementan considerando los controles y medidas de seguridad de la información que permitan garantizar su disponibilidad, integridad y confidencialidad, así como atendiendo las disposiciones establecidas en el Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento y sus normas reglamentarias.

Artículo 115. Pruebas para evaluar vulnerabilidades

115.1 Las entidades públicas planifican y realizan pruebas para evaluar vulnerabilidades a los siguientes activos: aplicativos informáticos, sistemas, infraestructura, datos y redes, que soportan los servicios digitales, procesos misionales o relevantes de la entidad. La ejecución de dichas pruebas se realiza, como mínimo, una vez al año. El Centro Nacional de Seguridad Digital solicita a la entidad información sobre las pruebas realizadas o coordina con ella la realización de dichas pruebas.

115.2 Los resultados de las pruebas realizadas constan como información documentada por la entidad. La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, solicita dichos resultados en el marco de sus funciones de supervisión o cuando lo considere necesario para la gestión de un incidente de seguridad digital.

DS 017-2024-PCM. Decreto Supremo que aprueba el Reglamento de la ley 30999, Ley de Ciberdefensa

TÍTULO PRELIMINAR

DISPOSICIONES GENERALES

Artículo I. Objeto

El presente reglamento tiene por objeto establecer las disposiciones normativas para regular las capacidades de ciberdefensa, operaciones militares, y uso de la fuerza en y mediante el ciberespacio, entre otras disposiciones para preservar la seguridad nacional, a cargo de los órganos ejecutores del Ministerio de Defensa, dentro de su ámbito de competencia, en el marco de la Ley Nº 30999, Ley de Ciberdefensa (en adelante la Ley).

Artículo II. Finalidad

El presente reglamento tiene por finalidad garantizar que las capacidades nacionales mantengan la continuidad de sus operaciones a través de la protección en y mediante el ciberespacio de los activos críticos nacionales, recursos claves, la soberanía y los intereses nacionales frente amenazas o ataques, cuando estos afecten la seguridad nacional.

Artículo III. Marco jurídico aplicable

Las operaciones militares en y mediante el ciberespacio, cuando afecten la seguridad nacional, se sujetan a lo establecido en la Constitución Política del Perú, la legislación nacional y las normas del derecho internacional que resulten aplicables.

Artículo IV. Definiciones

Para efectos de la Ley y el presente reglamento se entiende de forma específica las siguientes definiciones:

a. Activos Críticos Nacionales (ACN): Es la establecida en el numeral 3.4 del artículo 3 del Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales (ACN), aprobado por Decreto Supremo Nº 106-2017-PCM.

b. Acto hostil en el ciberespacio: Es toda acción en y mediante el ciberespacio que atenta contra la seguridad nacional, soberanía, los intereses nacionales, los ACN/RC. Da derecho al ejercicio de la legítima defensa conforme a las reglas de enfrentamiento establecidas por la autoridad competente, de acuerdo con la normatividad vigente. Con frecuencia son no cinéticos, dificultando la determinación y atribución.

c. Amenaza en el ciberespacio: Todo acto fuente, circunstancia o evento de origen externo o interno con la capacidad potencial de generar, a través del uso de sistemas, herramientas cibernéticas o cualquier otro instrumento en y mediante el ciberespacio, efectos adversos, daños o perjuicios a la seguridad nacional, soberanía, los intereses nacionales, los ACN/RC (Entiéndase también como ciberamenazas).

d. Arma cibernética: Agente de software empleado para objetivos de interés militar como parte de una acción ofensiva en y mediante el ciberespacio. Entiéndase también como ciberarma.

e. Ciberespacio: Comprende el conjunto de redes interconectadas e interdependientes de infraestructura de tecnología de la información, que incluyen a internet, las redes de telecomunicaciones, sistemas aislados (redes, sistemas y dispositivos de almacenamiento de información no conectados a internet), software, información, los protocolos de transportes, la energía eléctrica, los sistemas informáticos, procesadores y controladores integrados, junto con las personas que interactúan con ellos, entiéndase también como entorno digital. Conceptualmente es un ámbito sin un espacio físico más allá de la jurisdicción de cualquier nación.

f. Ciberseguridad: Es la establecida en el inciso h) del artículo 3 del Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.

g. Incidente de seguridad digital: Es la establecida en el inciso e) del artículo 3 del Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.

h. Infraestructura: Es la establecida en el inciso 3.3, del artículo 3, del Decreto Supremo Nº 106-2017-PCM, Decreto Supremo que aprueba el Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales.

i. Intención hostil en el ciberespacio: Es toda acción que evidencia la voluntad o preparación para ejecutar un acto hostil en o mediante el ciberespacio que atente contra la seguridad nacional, la soberanía, los intereses nacionales, los ACN/RC. Al igual que los actos hostiles son con frecuencia no cinéticos, lo que dificulta su determinación y atribución.

j. Legítima defensa: Es el derecho que tiene el Estado, mediante el empleo de los componentes de ciberdefensa de los órganos ejecutores del Ministerio de Defensa, de

usar la fuerza en y mediante el ciberespacio para impedir, contener y/o neutralizar un acto o intención hostil, que atente o ponga en riesgo la Seguridad Nacional.

k. Marco de Seguridad Digital del Estado Peruano: Es la establecida en el artículo 31 del Decreto Legislativo Nº 1412, que aprueba la Ley de Gobierno Digital.

l. Operaciones militares en el ciberespacio: Es el empleo de las capacidades de ciberdefensa por parte de los órganos ejecutores del Ministerio de Defensa, de acuerdo con sus funciones y en el ámbito de sus respectivas competencias, contra las amenazas o ataques que atenten contra la seguridad nacional, la soberanía, los intereses nacionales y/o los ACN/RC. Entiéndase también como ciberoperaciones.

m. Operador de los Activos Críticos Nacionales - ACN: Es la establecida en el inciso 3.6, del artículo 3, del Decreto Supremo Nº 106-2017-PCM, Decreto Supremo que aprueba el Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales.

n. Recursos Claves: Es la establecida en el inciso 3.13 del artículo 3 del Decreto Supremo Nº 106-2017- PCM, Decreto Supremo que aprueba el Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales.

o. Reglas de enfrentamiento: Se entiende de acuerdo con lo establecido en el artículo 10 del presente reglamento.

p. Riesgo de Seguridad Digital: Es la establecida en el inciso g) del artículo 3 del Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.

q. Sector Responsable: Es la establecida en el inciso 3.5, del artículo 3, del Decreto Supremo Nº 106-2017- PCM, Decreto Supremo que aprueba el Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales.

r. Seguridad Digital: Es la establecida en el artículo 30 del Decreto Legislativo Nº 1412, que aprueba la Ley de Gobierno Digital.

s. Seguridad nacional: Es la situación en la cual el Estado tiene garantizada su independencia, soberanía e integridad y, la población los derechos fundamentales establecidos en la Constitución. Esta situación contribuye a la consolidación de la paz, al desarrollo integral y a la justicia social, basada en los valores democráticos y en el respeto a los derechos humanos.

t. Uso de la fuerza: Entiéndase por uso de la fuerza, a la actuación que realizan las Fuerzas Armadas, en y mediante el ciberespacio, con los medios y métodos que correspondan, los cuales se encuentran delimitados a lo que dispone el artículo 51 de la Carta de las Naciones Unidas, la ley de Ciberdefensa y las normas del Derecho Internacional de los Derechos Humanos y del Derecho Internacional Humanitario y demás normativa del derecho internacional aplicable.

u. Vulnerabilidades cibernéticas: Debilidad o ausencia de capacidad para la defensa cibernética que puede ser utilizada por una amenaza. Esto comprende, pero no se limita a, un diseño deficiente, errores de configuración o técnicas de codificación, debilidades tecnológicas o políticas de seguridad inadecuadas e inseguras.

Artículo V. Acrónimos

Para efectos del presente reglamento se aplican los siguientes acrónimos:

a. ACN: Activos críticos nacionales

b. RC: Recursos clave

c. REN: Reglas de enfrentamiento

d. JCCFFAA: Jefe del Comando Conjunto de las Fuerzas Armadas

e. COCID: Comando Operacional de Ciberdefensa

TÍTULO I

DE LA CIBERDEFENSA

CAPÍTULO I

DEL MINISTERIO DE DEFENSA

Artículo 1. Rol del Ministerio de Defensa en la Ciberdefensa

Para la gestión del marco de Seguridad Digital del Estado Peruano, en el ámbito de la defensa, el Ministerio de Defensa, dentro del alcance de sus funciones y competencias dirige, norma, supervisa y evalúa las disposiciones en materia de ciberdefensa.

El Ministerio de Defensa, es la entidad encargada de gestionar la ciberdefensa. Asimismo, dicta políticas y lineamientos para el planeamiento y conducción de operaciones militares en y mediante el ciberespacio conforme a la Política de Seguridad y Defensa Nacional aprobada por el Consejo de Seguridad y Defensa Nacional y de manera articulada con los objetivos de seguridad nacional y con la Política Nacional de Transformación Digital, aprobada mediante el Decreto Supremo Nº 085-2023-PCM u otra norma que lo sustituya.

CAPÍTULO II

DE LOS ÓRGANOS EJECUTORES DEL MINISTERIO DE DEFENSA EN MATERIA DE CIBERDEFENSA

Artículo 2. Órganos Ejecutores del Ministerio de Defensa y componentes de ciberdefensa

Los órganos ejecutores del Ministerio de Defensa están constituidos por el Ejército, la Marina de Guerra, la Fuerza Aérea, y el Comando Conjunto de las Fuerzas Armadas.

La ciberdefensa comprende al COCID, y a sus componentes de ciberdefensa que son: el componente

de Ciberdefensa del Ejército del Perú, componente de Ciberdefensa de la Marina de Guerra del Perú y componente de Ciberdefensa de la Fuerza Aérea del Perú, los cuales ejecutan operaciones de ciberdefensa en y mediante el ciberespacio.

Artículo 3. Responsabilidades del Comando Operacional de Ciberdefensa

Son responsabilidades del COCID los siguientes:

a. Planear, organizar y conducir las operaciones militares en y mediante el ciberespacio, ejerciendo el comando y control de las operaciones de ciberdefensa conjuntas.

b. Proteger sus sistemas de información y el segmento del ciberespacio asignado.

c. Gestionar el registro de incidentes, el intercambio de información sobre ataques informáticos y patrones de amenazas entre los componentes de ciberdefensa de las Instituciones Armadas. Dicho registro es interno y de uso exclusivo del COCID, y tiene relevancia únicamente para las operaciones que realicen las Fuerzas Armadas.

d. Otras que se asignen en la normativa legal sobre la materia.

Artículo 4. Responsabilidades de los componentes de ciberdefensa de las Instituciones Armadas

Son responsabilidades de los componentes de ciberdefensa de las Instituciones Armadas las siguientes:

a. Planear, organizar y conducir a su nivel las operaciones militares en y mediante el ciberespacio, ejerciendo el comando y control de las operaciones de ciberdefensa propias.

b. Proteger sus sistemas de información y el segmento del ciberespacio propio o asignado.

c. Alistar integralmente a las unidades a su cargo, para el eficiente desempeño de sus funciones.

d. Desarrollar y mantener un óptimo nivel de sus capacidades de ciberdefensa.

e. Otras que se asignen en la normativa legal sobre la materia.

CAPÍTULO III

CAPACIDADES DE CIBERDEFENSA

Artículo 5. De las medidas pasivas y activas de ciberdefensa

5.1 Medidas pasivas en ciberdefensa: conjunto de actividades de prevención, protección y resiliencia del ciberespacio propio y/o asignado. Son de aplicación constante y generalizada, abarcando al personal, medios y sistemas propios o asignados. Involucra, pero no se limita al monitoreo de redes propias o asignadas, mantenimiento de sistemas informáticos, actualizaciones de seguridad y operativas, establecimiento de políticas, disposiciones, procedimientos y reglas de seguridad institucional, robustecimiento en la infraestructura cibernética propia y la concientización en materia de ciberdefensa, entre otras.

5.2 Medidas activas en ciberdefensa: conjunto de actividades de naturaleza proactiva, reactiva o de recuperación, en o mediante el ciberespacio propio, asignado y/o de interés. Estas medidas se aplican ante la necesidad militar para la defensa y la seguridad nacional. Involucra, pero no se limita al análisis de vulnerabilidades, una intensa labor de detección, evaluación, identificación y reconocimiento de actos hostiles o amenazas en el ciberespacio; o la aplicación de acciones cibernéticas sobre medios o sistemas que constituyen una amenaza, para degradar o neutralizar sus capacidades y formas de acción, a fin de impedir que estas puedan afectar la libertad de acción en el ciberespacio propio, asignado y/o de interés, entre otras.

Artículo 6. Capacidades de ciberdefensa de los Órganos Ejecutores del Ministerio de Defensa

En el ámbito de sus competencias, el COCID y los Componentes de Ciberdefensa de las Instituciones Armadas cuentan con las capacidades siguientes:

a. Capacidad de Defensa: consiste en la prevención, protección y resiliencia de las diferentes plataformas tecnológicas o sistemas de información ante amenazas cibernéticas, actos hostiles u otros incidentes de seguridad digital; recurriendo a medidas pasivas y activas.

b. Capacidad de explotación: consiste en la búsqueda, identificación, reconocimiento, vigilancia y seguimiento de ciberamenazas en y mediante el ciberespacio; recurriendo a medidas pasivas y activas.

c. Capacidad de respuesta: consiste en limitar o negar, temporal o permanentemente, el uso del ciberespacio del objetivo militar mediante la degradación o neutralización de sus sistemas, impactando en sus capacidades; recurriendo a medidas activas.

d. Capacidad de investigación digital o Investigación Forense Digital: consiste en el análisis de evidencia digital con la finalidad de determinar su funcionalidad, comportamiento, origen e impacto; así como su explotación futura a través de un proceso de ingeniería inversa.

Engloba técnicas de investigación y análisis forense digital para recolectar, analizar y preservar evidencias sobre actos maliciosos en el ciberespacio, recurriendo a medidas pasivas y activas. Esta capacidad de ciberdefensa se ejerce de acuerdo a las competencias asignadas, la cual no se vincula ni contrapone con la Investigación Digital que pueda realizar cualquier otra entidad pública o privada.

CAPÍTULO IV

OPERACIONES MILITARES EN Y MEDIANTE EL CIBERESPACIO

Artículo 7. De las Operaciones Militares en y mediante el ciberespacio

Comprende el conjunto de acciones orientadas, planificadas, organizadas y coordinadas para ser ejecutadas en y mediante el ciberespacio, con la finalidad de generar los efectos militares deseados para la seguridad nacional.

Con el empleo de las capacidades de ciberdefensa en las operaciones militares, articuladas sistémicamente por los componentes de ciberdefensa, de acuerdo a sus funciones y en el ámbito de sus respectivas competencias, contra las amenazas o ataques cuando estos afecten la Seguridad Nacional. Entiéndase también como ciberoperaciones.

CAPÍTULO V

DEL USO DE LA FUERZA EN Y MEDIANTE EL CIBERESPACIO

Artículo 8. Del uso de la fuerza en las operaciones de Ciberdefensa

8.1 Los componentes de ciberdefensa de las Instituciones Armadas recurren al uso de la fuerza en y mediante el ciberespacio para degradar o neutralizar las capacidades y formas de acción del adversario, que afecten la libertad de acción propia en el ciberespacio, ante la necesidad militar para la Defensa y la seguridad nacional.

8.2 El uso de la fuerza en y mediante el ciberespacio sólo se atribuye a los componentes mencionados en el párrafo precedente en operaciones militares bajo la conducción del JCCFFAA, de conformidad con lo dispuesto en las normas de Derecho Internacional de Derechos Humanos, del Derecho Internacional Humanitario y demás normativa del derecho internacional aplicable.

Artículo 9. Autorización para el uso de la fuerza

La autorización para el uso de la fuerza en las operaciones militares en y mediante el ciberespacio que atente contra la seguridad nacional está sujeta a disposición expresa, por parte del Presidente de la República, Jefe Supremo de las Fuerzas Armadas, que se efectúa por medio de Resolución Suprema refrendada por el Ministro de Defensa, y se ejecuta a través de los procedimientos establecidos para las otras operaciones militares, conforme a la normativa establecida para tal fin.

Artículo 10. Reglas de enfrentamiento

Son instrucciones emitidas por el JCCFFAA, mediante los cuales se mantiene el control sobre el uso de la fuerza por parte de las Fuerzas Armadas durante la ejecución de las operaciones militares en y mediante el ciberespacio ante un acto hostil e intención hostil que afecten la seguridad nacional. Se aprueban por Resolución Suprema refrendada por el Ministro de Defensa.

Artículo 11. Finalidades de las reglas de enfrentamiento

Las REN comprenden las siguientes finalidades:

a. Legal. Las REN constituyen un medio para asegurar que la actuación militar se sujete al marco jurídico vigente, tanto nacional como internacional durante la ejecución de las operaciones militares en y mediante el ciberespacio.

b. Militar. Las REN sirven de guía a los comandantes en lo referido al uso de la fuerza, durante la ejecución de las operaciones militares en y mediante el ciberespacio, estableciendo límites a su accionar.

c. Política. Las REN son una forma de asegurar que las Fuerzas Armadas actúen según los lineamientos políticos del nivel estratégico, vinculados al estado final deseado.

Artículo 12. Requerimiento, autorización o negación e implementación de las reglas de enfrentamiento

12.1 Cuando resulte necesario, el comandante militar que conduce las operaciones en y mediante el ciberespacio, puede requerir ante su superior inmediato la implementación, modificación o cancelación de alguna REN, a través del mecanismo de solicitud formal establecido por el JCCFFAA.

12.2 El comando superior que recibe la solicitud de implementación, modificación o cancelación de alguna REN se encuentra facultado para autorizar o denegar dicha solicitud, empleando los mecanismos formales establecidos por el JCCFFAA. Asimismo, el comando superior que recibe la solicitud, se encuentra facultado a incorporar restricciones adicionales a las REN liberadas.

Artículo 13. De la responsabilidad y su exención

Los supuestos de exención de responsabilidad penal derivados del uso de la fuerza durante las operaciones militares en y mediante el ciberespacio en aplicación de la Ley Nº 30999, Ley de Ciberdefensa y el presente reglamento son regulados conforme con lo establecido en los incisos 8 y 11 del artículo 20 del Código Penal.

TÍTULO II

DE LA SEGURIDAD DE LOS ACTIVOS CRÍTICOS NACIONALES Y RECURSOS CLAVES

CAPÍTULO I

DE LA PROTECCIÓN DE CONTROL DE LOS ACN/RC

Artículo 14. Protección y control de los activos críticos nacionales y recursos claves en y mediante el ciberespacio

14.1 Se considera que la seguridad digital de los ACN/ RC es afectada cuando se genera un ataque directo o inminente a sus recursos, infraestructura y sistema en sus componentes

digitales, por la materialización de riesgos derivados de amenazas y vulnerabilidades en y mediante el ciberespacio, y que generen como consecuencia daños a la persona, prosperidad económica, social y la seguridad nacional.

14.2 En el ámbito de la seguridad nacional, cuando la capacidad de protección en el ciberespacio de los operadores de los ACN/RC, del sector responsable de cada uno de ellos y/o de la Dirección Nacional de Inteligencia (DINI) sean sobrepasados, la protección y control de los mismos está a cargo del COCID, siguiendo el protocolo señalado en el artículo 16 del presente reglamento, con la finalidad de mantener las capacidades nacionales.

CAPÍTULO II

DE LOS PROTOCOLOS DE ESCALAMIENTO, COORDINACIÓN, INTERCAMBIO Y ACTIVACIÓN PARA LA PROTECCIÓN DE LOS ACN/RC

Artículo 15. De los responsables y etapas para la protección de los ACN/RC

La protección de los ACN/RC en y mediante el ciberespacio se realiza a través de los siguientes responsables y etapas:

15.1 En un primer momento, la ciberseguridad del ACN/RC está a cargo de su propio operador para preservar la Seguridad Digital, en cumplimiento de la normatividad vigente en seguridad y confianza digital; asimismo, coordina con el sector responsable y la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital o la que haga sus veces.

15.2 En un segundo momento, a su solicitud, cuando se presente un incidente que no pueda ser gestionado por el operador o supere sus capacidades, la Dirección Nacional de Inteligencia (DINI) complementa la capacidad de ciberseguridad del operador del ACN/RC, en coordinación con la Presidencia del Consejo de Ministros, a través de la

Secretaría de Gobierno y Transformación Digital o la que haga sus veces.

15.3 En un tercer momento, a su solicitud, cuando la capacidad de ciberseguridad de los Operadores de los ACN/RC, el sector responsable y la DINI sea sobrepasada, el Ministerio de Defensa, a través del Comando Conjunto de las Fuerzas Armadas y el COCID complementa las capacidades de ciberseguridad con sus capacidades de ciberdefensa.

15.4 En un cuarto momento, la Secretaría de Gobierno y Transformación Digital o la que haga sus veces, a través del Centro Nacional de Seguridad Digital, en el marco de sus competencias establecidas en el Decreto de Urgencia Nº 007-2020, ejerce sus propias facultades y/o acude a la asistencia nacional e internacional en materia de Seguridad Digital cuando las capacidades de ciberseguridad y ciberdefensa nacionales hayan sido sobrepasadas. La asistencia internacional complementa las capacidades de Ciberseguridad de los operadores de los ACN/RC, el sector responsable, la DINI y las capacidades de ciberdefensa de los órganos ejecutores del Ministerio de Defensa.

Artículo 16. Sobre el Protocolo de escalamiento, coordinación, intercambio y activación de incidentes de seguridad digital

16.1 El Protocolo de escalamiento, coordinación, intercambio y activación, debe incluir los procedimientos detallados, criterios y condiciones para la identificación y cambio de momento a los cuales se refiere el artículo precedente, así como la asignación de responsabilidades y la cadena de autoridad apropiada, de acuerdo a la normativa legal vigente.

16.2 El Protocolo de escalamiento, coordinación, intercambio y activación debe ser legible para humanos y adecuados para su uso mediante plataformas digitales o aplicaciones informáticas que automaticen el intercambio de información.

16.3 La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital o la que haga sus veces, elabora y emite el Protocolo de escalamiento, coordinación, intercambio y activación de incidentes de seguridad digital de los ACN/RC, de conformidad con lo establecido en el artículo 13 de la Ley.

16.4 Cuando algún incidente de seguridad digital comprometa los ACN/RC, se ejecuta el Protocolo de escalamiento, coordinación, intercambio y activación a través de las Directivas y/o lineamientos emitidos por la Secretaría de Gobierno y Transformación Digital o la que haga sus veces.

16.5 El referido protocolo se ejecuta con la comunicación directa e inmediata desde la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital o la que haga sus veces, al titular o representante del sector correspondiente.

DISPOSICIONES COMPLEMENTARIAS FINALES

Primera. Entrenamiento de capacidades en ciberdefensa

Los Órganos Ejecutores del Ministerio de Defensa establecen de manera permanente ejercicios en ciberdefensa con la finalidad de entrenar las capacidades en ciberdefensa.

Segunda. Protocolo de escalamiento, coordinación, intercambio y activación de incidentes de seguridad digital

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital o la que haga sus veces, emite los protocolos de escalamiento, coordinación, intercambio y activación de incidentes de seguridad digital de los ACN/RC, en un plazo no mayor a ciento ochenta (180) días hábiles contados a partir del día siguiente de la publicación del presente Reglamento.

ÍNDICE


LaSalle
Universidad